AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

EVALUATING THE SECURITY OF THE U.S. FINANCIAL SECTOR

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

JUNE 24, 2015

Printed for the use of the Committee on Financial Services

Serial No. 114–36

U.S. GOVERNMENT PUBLISHING OFFICE

96–997 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:	
June 24, 2015	1
Appendix:	
June 24, 2015	39

WITNESSES

WEDNESDAY, JUNE 24, 2015

Carlson, John W., Chief of Staff, Financial Services Information Sharing and Analysis Center (FS-ISAC)	10
Poncy, Chip, Senior Advisor, Center on Sanctions and Illicit Finance at the Foundation for Defense of Democracies, and Founding Partner, Financial Integrity Network	8
Vance, Hon. Cyrus R., Jr., District Attorney, New York County	6

APPENDIX

Prepared statements:	
Carlson, John W.	40
Poncy, Chip	60
Vance, Hon. Cyrus R., Jr.	81

ADDITIONAL MATERIAL SUBMITTED FOR THE RECORD

Ellison, Hon. Keith:	
Article from the New York Times entitled, "Homegrown Extremists Tied to Deadlier Toll Than Jihadists in U.S. Since 9/11," dated June 24, 2015	86
Southern Poverty Law Center Hate Map (Active U.S. Hate Groups by State)	89
Written responses to questions for the record submitted to John W. Carlson	90

EVALUATING THE SECURITY OF THE U.S. FINANCIAL SECTOR

Wednesday, June 24, 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 2:30 p.m., in room 2128, Rayburn House Office Building, Hon. Michael Fitzpatrick [chairman of the task force] presiding.

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

Ex officio present: Representative Waters,

Chairman FITZPATRICK. Thank you everyone for joining us today for the third hearing of the House Financial Services Committee's Task Force to Investigate Terrorism Financing. Today's hearing is entitled, "Evaluating the Security of the U.S. Financial Sector."

Through the first hearings of this task force, we have heard about the extensive reach—both in terms of impact and funding—of the terror groups that the United States and allied nations face today. From the Middle East to South America, we have examined the new methods of financing that these organizations are utilizing to spread and carry out their warped ideological aims.

Terrorist groups no longer rely solely on "big-pocket donors," or even state sponsors, but have diversified their streams of revenue to include a wide array of activities. Non-traditional funding methods—from antiques dealing and the sale of illicit oil in Iraq and Syria, to the drug trade and extortion in the Tri-Border Area of Argentina, Brazil, and Paraguay—have transformed these groups from regional entities to trans-national criminal syndicates.

With this global scope, it is vital that the United States works with the international community to address these challenges. However, it is equally important that we look inward to assess the security of our own financial sector.

That is the focus of today's hearing.

Many groups are constantly seeking to access and exploit the U.S. financial system. The complexity and sheer size of our financial system has created avenues within which criminals may move, hide, and launder their funds. Many of these groups understand our system's weaknesses and gray areas with respect to beneficial ownership and customer due-diligence standards and they exploit it to our detriment.

Aside from the threat of actors operating within it, the United States financial system itself should also be considered a target for terrorists.

Over the past several years, there has been a noticeable rise in the number of cyber-related attacks on United States businesses and government agencies, launched by state and non-state actors alike. This is attributed to the fact that such attacks cost very little to carry out, but have potential to cause severe problems and inflict great costs on the victim attempting to carry out the defense.

The United States financial sector is too important for this task force to overlook when seeking to address the nexus of terrorism and finance. The continued innovation and evolution by our enemies highlights the importance of this body's role in the fight against terror.

The United States must do better when defending our financial system and addressing the threats operating within it. The risk is too great to ignore.

I am confident that today's dialogue between this bipartisan group of Members and the panel of expert witnesses that we have before us will help us to understand where our system is vulnerable and how these vulnerabilities should be corrected.

At this time, I would like to recognize for 3 minutes the task force's ranking member, my colleague from Massachusetts, Mr. Lynch, who has been a valuable asset to the task force.

Mr. LYNCH. Thank you, Mr. Chairman. I want to thank the members of the panel as well, the witnesses, for helping the task force with its work.

This is our third hearing. The first two were focused on the global reach of anti-terrorist financing. And I look forward to this third hearing which is going to actually look at the opportunity to evaluate the domestic security of the U.S. financial sector in order to better protect it from terrorist threats.

It is an inward-focused perspective which I think is eminently necessary. It is crucial that our task force, as part of the Financial Services Committee, devotes resources to assessing the security of the U.S. financial sector. As our witnesses highlighted in their prepared remarks, the size and complexity of the financial sector makes it vulnerable for abuse by terrorist organizations.

Shell companies and vulnerabilities in our financial system's cyber infrastructure are two areas that are particularly susceptible to exploitation by terrorists.

Shell companies particularly are being used to mask the identities of people who actually control or profit from these companies, the beneficial owners. And unfortunately, the United States does not currently collect information on beneficial owners.

As Mr. Vance, a seasoned New York County district attorney, described in his prepared remarks, criminals and terrorists exploit our inadequate incorporation procedures and the anonymity in those procedures in order to conceal the illicit conduct. This makes it hard for law enforcement to follow the money to the ultimate owner.

At this point, I want to yield to Mr. Brad Sherman of California for a brief opening statement.

Mr. SHERMAN. I have a very quick statement that relates to the chairman's comments about cyberattacks from state actors. It is a step away from the exact focus of the hearing.

The best defense against state actors attacking our cyber system is a good offense. We are too politically correct to have a good offense. We only go after government targets, we only take the information for government files.

China is uniquely vulnerable to us if we choose to be politically incorrect. What we need to do is gather information about the assets and expenditures of their top 1,000 governmental officials, none of whom, I might add, are reported on personal financial disclosure statements filed with the ethics committee of any parliament. And if we were to expose even a few of the tasty tidbits, China would no longer be hacking into our system.

But that is not politically correct. We will have bureaucrats asking us for money. They will only want to spend money on defense; they are a little wary of offense. And so, we will continue to be a punching bag, trying only to defend ourselves.

I yield back.

Mr. LYNCH. I would like to also yield 1 minute for a brief statement to Ms. Sinema of Arizona.

Ms. SINEMA. Thank you, Chairman Fitzpatrick, and Ranking Member Lynch.

The Administration has identified the financial services sector as critical infrastructure integral to our national security. Cyberattacks on U.S. critical infrastructure, including the financial sector, come from states, terrorists, criminals, and hacktivists.

Sharing information about cyber breaches and threats is critical to ensuring the financial institutions and affected parties effectively prepare for and respond to cyberattacks. However, this doesn't always occur.

Firms and industry groups have cited concerns over violating privacy and antitrust laws as a reason that they are reluctant to share information. So we must make it easier for the private sector to successfully access threat information and remove barriers to sharing within the private sector and with the Federal Government.

Information sharing is an important tool for protecting information systems and their contents from unauthorized access from cyber criminals. But it is only one of the many assets of cybersecurity that organizations must address to secure their systems and information.

I am looking forward to continuing to work with my colleagues on both sides of the aisle to reduce vulnerabilities in the cybersecurity ecosystem and strengthen measures to protect our critical infrastructure. And I am looking forward to hearing more from our witnesses today about the essential elements of effective cyberthreat information-sharing legislation.

Thank you. I yield back.

Chairman FITZPATRICK. I now recognize the vice chairman of the task force, Mr. Pittenger of North Carolina, for 1 minute for the purpose of making an opening statement.

Mr. PITTENGER. Thank you, Mr. Chairman.

And thank you to Ranking Member Lynch for your continued efforts with this task force.

Recent reports from the State Department and the Treasury Department have further highlighted the priority that we must place in our counter-terrorist financing efforts.

The 2014 State Department Country Reports on Terrorism make it clear that terrorism is becoming more prevalent. The number of attacks increased by 35 percent with 3,000 more attacks in 2014 than 2013, and fatalities increased 81 percent to 32,727 deaths in 2014.

And the National Terrorist Financing Risk Assessment shows that while we have made progress in undermining terrorist financing, there are still vulnerabilities in our system and more could be done.

While the United States is in compliance with the majority of the Financial Action Task Force (FATF) recommendations, we have our own noncompliance issues. I look forward to continuing to work with this task force to achieve this, including efforts to increase the cooperation between the public and the private sector.

I look forward to the testimony today and the views of our distinguished witnesses on what else can be done to stop the flow of money to terrorists.

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

Chairman FITZPATRICK. We now welcome our witnesses. And I recognize the gentleman from New York, Mr. King, for the purpose of introducing the district attorney of New York County.

Mr. KING. Thank you, Mr. Chairman. Thank you for giving me this privilege because it really is a privilege to introduce Cy Vance to this committee.

Cy Vance comes from a tradition of district attorneys in New York where his two predecessors, Frank Hogan and Robert Morgenthau, between the 2 of them served for more than 65 years. So this is a very distinguished office and Cy Vance more than fits the bill; he more than lives up to the standards of that office.

He was elected in 2009. He was re-elected with 91 percent of the vote in 2013. All of us can only envy that vote margin. But before that, he was a leading prosecutor and also had a very successful career in the private sector.

The main reason he is uniquely qualified today is that his office, the district attorney's office located in the world financial capital, has been extremely active in international financial issues, recovering billions of dollars from institutions that have violated sanctions, and on the issue of terrorism itself; he was the first district attorney to obtain a terrorist conviction in New York State courts.

It was the Pimentel case which other prosecutors, including the Federal Government, did not want to go near because they thought it could not be won. The fact is a conviction was obtained and it was a very, very significant conviction for the district attorney. So I look forward to District Attorney Vance's testimony here today. I can tell you—I am saying this as a Republican—that he is universally respected in New York by all political parties, by members of the bar, by police, by law enforcement, and by defense counsel. And his testimony today will be extremely illuminating and helpful.

And Cy, it is a real privilege to have you here today.

Mr. Chairman, I yield back.

Chairman FITZPATRICK. Thank you.

Welcome to the panel, Mr. Vance.

Next, we have Chip Poncy, a founding partner of the Financial Integrity Network, and a senior adviser of the Center on Sanctions and Illicit Finance at the Foundation for Defense of Democracies.

Mr. Poncy previously served as the interim head of financial crimes compliance from Mexico and the Latin American region for one of the world's largest banks. Mr. Poncy also served as the inaugural director of the Office of Strategic Policy for Terrorist Financing and Financial Crimes and as a senior adviser at the U.S. Department of the Treasury.

From 2010 to 2013, Mr. Poncy led the United States delegation to the Financial Action Task Force where he co-chaired a policy working group and managed United States participation on illicit finance expert groups.

Mr. Poncy graduated with honors from Harvard University, received a masters degree in international relations from the Johns Hopkins School of Advanced International Studies, and holds a law degree from the Georgetown University Law Center.

He also graduated from high school with Representative Rooney of Florida, further distinguishing himself.

So, we welcome you.

And finally, we have John Carlson, the chief of staff at the Financial Services Information Sharing and Analysis Center, or the FS-ISAC.

Prior to joining the FS-ISAC, Mr. Carlson served as the executive vice president of BITS, the Technology and Policy Division of the Financial Services Roundtable. There, Mr. Carlson led cybersecurity, technology, and collaboration programs for 12 years and participated in the Financial Services Sector Coordinating Council.

Mr. Carlson also served as managing director of Morgan Stanley's Operational Risk Department and in a variety of leadership roles at the Office of the Comptroller of the Currency, the Office of Management and Budget, the Federal Reserve Bank of Boston, and the United Nations Center for Human Settlements.

Mr. Carlson graduated from the University of Maryland, and received a masters degree in public policy from the Kennedy School of Government at Harvard University.

The witnesses will now be recognized for 5 minutes each to give an oral presentation of their 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 that you are speaking directly into it.

With that, Mr. Vance, you are now recognized for 5 minutes. Just make sure the microphone is turned on as well.

STATEMENT OF THE HONORABLE CYRUS R. VANCE, JR., DISTRICT ATTORNEY, NEW YORK COUNTY

Mr. VANCE. Good morning, Chairman Fitzpatrick, Ranking Member Lynch, Representative King, and members of the Task Force to Investigate Terrorism Financing.

As the head elected law enforcement official for New York County, which is a target for terrorism from around the world, I want to thank you for taking on this crucial issue, and for the opportunity to talk to you and with you today.

I came to share with you the perspective of State and local law enforcement on nontransparent beneficial ownership and the ease with which criminals and terrorists can operate anonymously in our jurisdictions.

As Representative King indicated, because of my office's location in Manhattan as a global financial capital, our office has the responsibility to interrupt terrorism financing and other financial crime. And for decades, our office has conducted investigations that rely on financial tracing and analysis to root out these crimes along with money laundering, sanctions violations, human trafficking, cyber crime, and other frauds.

Like many in white-collar law enforcement, our way of doing business is to identify the money and to follow the money, which in most cases means issuing subpoenas for records from financial institutions and pursuing the leads that those records provide. But sometimes those records lead nowhere.

I want to share an anecdote which should be disturbing. It is not, unfortunately, uncommon.

While I was preparing for my testimony here, an investigator in my office entered the phrase "incorporate Delaware company" into a Google search. And she called an incorporation services vendor that appeared in her search results.

Putting on her best accent, she stated that she lives in France, that she wanted to incorporate a company in Delaware, but that she wished to remain anonymous because of "estate issues" in her country. And she was told that wouldn't be a problem. A corporation could be set up in 5 minutes; she needed to provide only a name and an email address.

And that interchange, I believe, highlights starkly what I and my colleagues know very well: That criminals currently can and do make use of our lax incorporation procedures and the anonymity those procedures permit in order to carry out and conceal illegal conduct.

On a nearly daily basis, we encounter a company or a network of companies involved in suspicious activity, but we are unable to glean who is actually controlling and benefiting from those entities and from their illegal activity. In other words, we cannot identify the criminal.

And that is not because entities are incorporated in an offshore tax haven like the Cayman Islands. That country actually collects beneficial ownership information. Often, that entity is instead incorporated in the United States, and it is incorporated in the United States precisely because we don't collect beneficial owner information.

And in this important way, a prosecutor sitting in the Cayman Islands is better positioned to root out terrorism finance in her own markets than I am in ours.

Too frequently, an anonymous incorporation record spells the end to our investigative road. And when we are able with much time and effort to overcome that obstacle, we often find that the criminals have purposely relied on our lax incorporation requirements.

Recently, for example, a New York County grand jury indicted eight individuals in a sprawling pump-and-dump securities fraud scheme in which stock promoters and company insiders reverse-merged private companies with no publicly traded securities into existing public shell companies.

They concealed their control of the shell companies by using nominees to purchase them and to hold the publicly traded shares in their names. But the scheme's mastermind appears nowhere in the incorporation documents and held none of the company's shares in his name.

As in so many of our cases, disguised beneficial ownership is precisely what enabled this scheme.

The perils of anonymous incorporation go well beyond securities fraud. Shell companies doing business in New York can be used to disguise the activities of entire foreign governments.

In 2006, my office was investigating the Alavi Foundation, a not-for-profit organization which owned a 60 percent stake in a 36-story office building in midtown Manhattan. The remaining 40 percent was owned by the Assa Corporation, a New York incorporated entity, and by Assa Company Limited, which was incorporated in the Channel Islands.

We ultimately determined that the Assa entities were merely shells being used to disguise the building's actual owner, a bank called Melli. Bank Melli, as you may be aware, is wholly owned by the government of Iran. It was designated by the Office of Foreign Assets Control (OFAC) as a key financier to Iran's nuclear and ballistic missiles program and as a banker to the country, the Revolutionary Guard, and the Quds Force.

The building generated substantial rental income which was diverted to the shell companies and from there to Bank Melli.

My office routinely collaborates with foreign law enforcement to incapacitate cross-border threats. But time and time again, we find that our international partners are better situated to assist us in thwarting terrorism and financial crime than vice versa.

It is detrimental to those partnerships when we have to tell our international law enforcement friends that we can't assist them in taking down U.S.-incorporated terrorist enterprises because information about the owners of the entities formed in our own States is beyond our reach.

A simple requirement to identify beneficial owners on State incorporation forms would vastly improve the capacity of American law enforcement to attack terrorism finance and disrupt terror plots.

Thank you for the opportunity to testify today.

[The prepared statement of District Attorney Vance can be found on page 81 of the appendix.]

Chairman FITZPATRICK. Mr. Poncy, you are now recognized for 5 minutes.

STATEMENT OF CHIP PONCY, SENIOR ADVISOR, CENTER ON SANCTIONS AND ILLICIT FINANCE AT THE FOUNDATION FOR DEFENSE OF DEMOCRACIES, AND FOUNDING PARTNER, FINANCIAL INTEGRITY NETWORK

Mr. PONCY. Chairman Fitzpatrick, Vice Chairman Pittenger, Ranking Member Lynch, and other distinguished members of the task force, I am honored by your invitation to testify today, particularly with such a distinguished panel.

There are important steps that this task force can take to strengthen the security of our financial system, the integrity of our economic markets, and our national and collective security.

Such steps will help combat terrorism, transnational organized crime, WMD proliferation, and corrupt elites by denying these and other national security threats access to the financial services they require.

These steps will also strengthen our ability to identify, pursue, and disrupt illicit financing networks that fuel and enable these threats. These steps must focus on addressing systemic challenges to our financial integrity. Such challenges stem largely from weaknesses in implementing global anti-money-laundering and counter-terrorist financing standards, standards that U.S. leadership has helped create through the Financial Action Task Force, or FATF.

These global standards direct countries to implement comprehensive anti-money-laundering, counter-terrorist financing regimes that deliver financial transparency and financial accountability.

Financial transparency allows us to track and trace illicit financing across an increasingly globalized financial system. Financial accountability ensures that our financial institutions implement the systems and controls required to deliver financial transparency.

Financial accountability also ensures the aggressive pursuit, disruption, and deterrence of illicit financing activity, actors, and assets that infiltrate our system.

In an increasingly globalized financial system, economy and threat environment, we must pursue a global approach to achieving these objectives. Such an approach must build upon our success in leading the global implementation of the international framework for anti-money laundering and combating the financing of terrorism (AML/CFT) regimes that deliver financial transparency and accountability.

This requires legislation and rulemaking to close key gaps in implementing a number of FATF global standards essential to achieving financial transparency here at home.

It also requires continued aggressive enforcement and a strengthened partnership with the financial sector to facilitate compliance with financial transparency requirements. And it requires additional resources to expand targeting of illicit financing networks.

This committee can strengthen U.S. leadership in overcoming these challenges by taking the following 10 steps that will significantly enhance financial transparency and accountability.

One, adopt legislation expanding the purposes of the Bank Secrecy Act (BSA) to explicitly include protecting the integrity of the

financial system. Such legislation is required to underscore the importance of partnership with the financial institutions that comprise our financial system.

Two, adopt legislation to require the disclosure and maintenance of meaningful beneficial ownership information in our company formation processes. Such legislation is required to address the chronic abuse of legal entities that mask the identities and illicit financing activities of the full scope of criminal and illicit financing activities in actors.

Three, collaborate with the Treasury Department to consider legislation that strengthens the information-sharing provisions of Section 314 of the USA Patriot Act. Such action may assist in addressing systemic challenges to financial integrity posed by information-sharing constraints.

Four, support the issuance of Treasury's proposed rule on customer due diligence, consistent with that of standards. Such action is required to address the systemic challenges posed by CDD practices that fall below global standards here in the United States and particularly with respect to beneficial ownership.

Five, support Treasury's consideration to extend AML/CFT preventive measures to investment advisers and financial intermediaries and real estate transactions, consistent again with global standards.

This action is required to help address the systemic challenges created by gaps in our financial system that are not covered by AML/CFT regulation. This includes a blind spot with respect to more than $66 trillion of assets under management, held by investment advisers that currently sit outside the scope of AML/CFT regulation in our markets.

Six, support Treasury's consideration of lowering the recordkeeping and travel-rule thresholds, consistent with that of standards.

Seven, provide protective resources for Treasury to enhance examination and supervision of BSA-covered industries that lack a Federal functional regulator.

Eight, provide protective resources for the IRS and Department of Justice to enhance financial investigations of illicit financing networks. Such action is needed to strengthen the systemic pursuit of illicit financing networks of the criminal investigative and prosecutorial authorities that are the best suited and the best trained to support this mission.

Nine, provide protective resources for Treasury to enhance targeting of primary money-laundering concerns under Section 311 of the Patriot Act and targeting of illicit financing networks under national security authorities. Such action is needed to give the Treasury the resources it requires to continue applying targeted financial measures that effectively disrupt a growing range of criminal and national security threats.

And ten, provide protective resources for Treasury to develop foreign capacity in critical financial centers to support the effective implementation of targeted financial measures.

These 10 steps outline the foundation for an action plan that this committee can move forward with to strengthen our financial integrity and the effectiveness of our counter-illicit-financing mission.

Once again, I am honored to testify here today in support of those who, across our government and financial services industries, fight every day to protect our financial integrity. They are literally the best in the world in advancing this mission and their continued success will require your ongoing support. Thank you.

[The prepared statement of Mr. Poncy can be found on page 60 of the appendix.]

Chairman FITZPATRICK. Thank you.

Mr. Carlson, you are now recognized for 5 minutes.

STATEMENT OF JOHN W. CARLSON, CHIEF OF STAFF, FINANCIAL SERVICES INFORMATION SHARING AND ANALYSIS CENTER (FS-ISAC)

Mr. CARLSON. Great. Thank you very much, Mr. Chairman.

My name is John Carlson, and I am the chief of staff of the Financial Services Information Sharing and Analysis Center (FS-ISAC). FS-ISAC is a not-for-profit formed in 1999 in response to Presidential Decision Directive 63 of 1998.

My written statement includes some details on our 16-year history, our 6,000 member organizations, what we do, and how we engage with the United States and others around the globe.

Briefly, we play a critical role in sharing cyber and physical threat information, conducting coordinated contingency planning exercises, managing rapid response communications for both cyber and physical events, such as Hurricane Sandy of 2012, and fostering collaborations with other key sectors and government agencies.

Thank you for inviting me to testify today at this hearing on evaluating the security of the U.S. financial sector.

The current security threat environment continues to evolve and intensify. It affects all institutions regardless of size and type. Increasingly other sectors such as retailers and health care providers and, yes, even our own Federal Government, face these same threats.

We see malicious cyber actors with increasing sophistication and growing persistence. These actors vary considerably in terms of motivation and capability. They range from nation states conducting espionage and sponsoring what we call distributed denial of service (DDOS) attacks, advanced cyber criminals who seek to steal money, terrorists looking to finance their activities, and hacktivists intent on making political statements.

There are numerous tactics that malicious cyber actors use to target financial institutions. Among these, the following are concerning: targeted spear phishing campaigns; ransom-ware attacks; distributed denial of service attacks; a new one, business email compromise leading to fraudulent wire transfers; supply chain risks; a blending of physical and cyberattacks like we have seen in some of the attacks going after ATM networks; and of course, insider threats which oftentimes yield the most damaging results.

The quote often attributed to Willy Sutton that he robbed banks because that is where the money is, reminds us why financial institutions are often the subject of cyberattacks. However, that quaint quote does not capture the entirety of the situation we face today.

We are also observing that financial institutions are being targeted in response to international conflicts. Perhaps the best visible example of this was the DDOS attack several years ago when an organization backed by a foreign country targeted dozens of financial institutions over many months.

The persistent, organized attacks were very disruptive. The only silver lining is that they resulted in unprecedented levels of information sharing among financial institutions and with the U.S. Government.

For example, the information shared by firms that were attacked during the first wave benefited firms targeted during the second, third, and fourth waves. They also resulted in elevating cyber to a CEO-level issue, where it remains today.

The financial sector is increasingly concerned with the potential for attacks that could undermine the integrity of the financial system through data manipulation and destruction.

In response, my organization, working with others, has launched a task force with over 80 representatives from firms and government agencies to develop best practices on how to mitigate and respond to potential destructive malware attacks.

These are serious concerns and we are addressing them in a serious manner. We are investing in the future and fostering collaborations to better match the threat environment.

For example, last year we launched with the Depository Trust and Clearing Corporation, Soltra Edge, a game-changing new service that automates cyber threat information sharing. Soltra Edge leverages two open standards: the Structure Threat Information eXpression, or STIX; and the Trusted Automated eXchange and Indicator Information, also called TAXII, that the Department of Homeland Security funded and the MITRE Corporation developed.

I certainly don't want to leave you with the impression that the financial sector needs more regulation to address the cyber challenge. In my written statement, I explain the extent to which the financial sector is regulated based in part on the Gramm-Leach-Bliley Act of 1999, as well as extensive supervisory guidance that regulators have issued over the past 15 years.

I also explain how our sector's strong risk management culture and our leadership in collaborating with other sectors and government agencies is critical to our success in repelling these attacks.

Let me conclude by saying that the information-sharing practices that our sector uses today are working well to the point that other sectors are looking to us for guidance and best practices. However, much more needs to be done given the increasing risks our sector and country faces.

I outline in my written statement some recommendations for actions for the Congress and the Administration that could supplement these efforts. In short, the Congress can play a constructive role by enacting cyber-threat information-sharing legislation, which I know the House has passed, and it is awaiting action in the Senate; encouraging financial regulators to harmonize regulatory requirements; and supporting other efforts by the Administration to enhance information sharing and cyber protections.

Thank you for the opportunity to testify.

[The prepared statement of Mr. Carlson can be found on page 40 of the appendix.]

Chairman FITZPATRICK. We thank the panel of expert witnesses for your opening statements here to the task force.

At this point, each of the Members will be recognized for 5 minutes for the purpose of asking questions.

I now recognize myself for questions.

Mr. Poncy, in your testimony you mentioned actions, and you have mentioned this in the past as well, actions that could be taken by the United States to meet the FATF global standards, customer due diligence rule, you have mentioned lowering the travel record-keeping threshold from $3,000 to $1,000. What are the obstacles the United States Treasury Department is encountering which are prohibiting adoption of some of these rules at this point? Is it lack of resources? Is it political will? What do you believe it is?

Mr. PONCY. Thank you, Congressman. Two great questions, and I think the answer is a combination of a lack of understanding of the importance of those rulemakings to protecting our financial integrity, and a stretch of resources that are required to advance our counter-illicit-financing mission.

The Treasury Department, the investment of the Treasury Department to manage the security of the financial system is a fraction of the investment that is made across our national security infrastructure. That is no secret. Main Treasury is very small. It operates like a professional firm.

It also has responsibility to manage the integrity of not just the U.S. financial system, but in today's globalized economy, pretty much the global financial system. The people at the Treasury Department work harder than any of the folks that I have worked with throughout my career.

To ask them to continue the expansion of this mission, due to its success, what started as a counterterrorism financing campaign built on the back of AML systems and has now expanded to include threats against transnational organized crime, WMD proliferation, grand-scale corruption, cyber crime, is being done with the same group of people who were working 24-hour shifts to combat terrorism financing after 9/11. They need more resources. It is just that simple.

But in addition to that, they need support, not only of the Congress, but of the general public. The American Bankers Association and the American Bar Association have been visibly absent from supporting Treasury's role in customer due diligence. This is evident in the comments with respect to the rulemakings that Treasury has proposed.

Some of the concerns they have raised are important concerns. Treasury has engaged in historic outreach on these rulemakings. In the 40-year history of the BSA, the Treasury Department had never conducted a cross-country campaign in New York, Washington, Miami, Chicago, or L.A. with banks, with broker dealers, with insurance companies, with futures commissions merchants, with money service businesses, to understand the challenges of implementing customer due diligence and to get it right.

I would submit that the proposed rule that Treasury issued last July gets it right. Getting that rule from a proposed rule to a final rule requires more visibility and more support from the Congress and from the general public. Thank you.

Chairman FITZPATRICK. Mr. Vance, you have been one of the Nation's leaders ringing the bell on the whole issue of beneficial ownership. You are doing it as a law enforcement professional working with mainly State, city, county, and other law, and there is some intersection with Federal agencies.

Recently, the Treasury issued a notice of rulemaking on this subject of beneficial ownership. I was wondering if you were familiar with that notice and if you have any comments on that?

Mr. VANCE. In all honesty, Congressman, I am not familiar with it in detail, so I don't want to mislead you before I answer the question.

Chairman FITZPATRICK. What it would do, is ease compliance burdens compared with the advanced notice of proposed rulemaking which would have forced institutions to verify that beneficial owners listed by an account holder were actually the entity's beneficial owner.

Mr. VANCE. Congressman, our issue is our ability to access that information for State prosecutors. So if we have to go to the IRS, for example, to get that information, current law does not permit us to just go to the IRS and obtain information that we can then use to investigate.

So I think that is a step, but my preference, as I indicate in my testimony, is that there be a 50-State solution to this whereby beneficial ownership is required upon incorporation and that will give prosecutors like myself equal and direct access through grand jury subpoenas to information that is vital for us to protect our communities.

Chairman FITZPATRICK. I am going to ask each of you, if you can make one suggestion on the issue of information sharing, we will start with Mr. Carlson, a suggested amendment or change to Section 314 of the USA Patriot Act, what would it be?

Mr. CARLSON. I don't know the specifics on Section 314, but I think in general we are looking for protections to share information so you are not held liable for sharing that information, as well as protections from disclosure, such as the Freedom of Information Act, if you are sharing information with the government.

I think within the financial sector, we actually have developed a mechanism to share that kind of information, but we need further protections in order to encourage others to start sharing and to give them some legal cover in case they do share and that information gets released.

Chairman FITZPATRICK. Mr. Poncy, could you quickly suggest a recommendation?

Mr. PONCY. Thank you, Congressman. There are two elements of Section 314 that bear re-examination. One is that 316B allows financial institutions to share information related to combating financial crime and achieving safe harbor from different types of liability associated with information sharing.

But the type of information sharing that is anticipated under 314 is not necessarily the most expansive imaginable. What we want,

what we need is to have our best compliance teams sitting in our global banks working with one another to map illicit financing networks.

We know a lot of people who do this. They used to do this at the Treasury Department. They used to do this at the FBI. They used to do this in the Manhattan DA's office. And they are some of the best investigators in this we have. They cannot sit down with one another with their customer data and link this up to figure out where illicit networks are penetrating our institutions.

So one is the kind of information sharing that we are talking about.

And two is what is a permissive allowance perhaps should be a requirement.

So those would be two suggestions to start.

Chairman FITZPATRICK. Thank you.

My time has expired.

I would like to recognize the ranking member of the full Financial Services Committee, Ms. Waters of California.

Ms. WATERS. Thank you very much.

I would like to address this question to Mr. Cyrus Vance.

The Patriot Act allowed FinCEN to temporarily exempt certain categories of entities and institutions from having to establish a basic anti-money-laundering program that entails developing internal policies, procedures, and controls, designating a compliance officer, providing for ongoing employee training, and an independent audit function to test programs.

Today, nearly 14 years after the Patriot Act was passed, there are a number of categories of institutions that remain exempt from these basic requirements. The list of exempted entities includes pawn brokers, travel agencies, sellers of vehicles, including automobiles, airplanes and boats, persons involved in real estate closings and settlements, private bankers, commodity pool operators, commodity trading and advisers, and investment companies.

Do you believe it is time for Treasury to revisit whether the exemptions for the entities I just listed continue to be appropriate?

Mr. VANCE. I do, Congresswoman. I think you answered your question by asking it. We have 5 years—much more experience now as a result of the Patriot Act and I think some of the categories of industry that you talk about are now ones that should be looked at in order to consider whether they should be included.

Ms. WATERS. Thank you very much.

Let me go to Mr. Poncy.

I understand that you were at Treasury, is that right?

Mr. PONCY. That is right, ma'am.

Ms. WATERS. And so the question that I just asked, could you please give us your take on that?

Mr. PONCY. Thank you very much. And I am always happy to have the Manhattan district attorney take the words out of my mouth. I couldn't agree more.

I certainly think it is time to re-examine it, but it is important how we do it.

The limited resources we have over our regulatory system are such that even for sectors that we have nominally regulated, we cannot ensure their integrity.

So we have at the moment BSA regulation requirements over high-priced commodity merchants and dealers. There is no Federal regulator over that. It is the same for money service businesses and insurance companies.

One of the recommendations that I have in my testimony is that we invest targeted resources to strengthen oversight of sectors that are already covered so that they actually understand and implement the obligations that are already on the books.

The second recommendation that I have in my testimony is to do exactly what you suggested, to examine the coverage of the financial system with existing requirements.

In particular, the investment adviser sector is one that controls $66 trillion of assets under management, that is "trillion," with a "t." That is 5 times our GDP. That sector does not have any AML/CFT obligations right now, so I would start there.

And then I have also recommended taking a look at financial intermediaries involved in real estate closings. All of us have seen the exposes in New York and Miami and elsewhere about high-luxury properties going to offshore interests often on the back of corrupt proceeds. If we want to stop those activities, then I suggest that we start with those two sectors in particular.

And I know the Treasury Department is strongly considering that. Again, it is a question of resources and a question of public visibility. So, support to the Treasury Department for what is already an effort to try to get ahead of this might help the Administration get over the fence.

Ms. WATERS. In your testimony, you also stated that the long string of U.S. enforcement actions against global banks and other financial institutions in recent years underscores the U.S. commitment to global anti-money-laundering and counterterrorism financing regime and financial integrity.

And then you say it also raises questions about the state of industry compliance and the cultural commitment to compliance on critical national security matters across the banking sector.

I want to tell you that I was very surprised. We spent quite a bit of time on HSBC Bank. And of course, there was a big fine against them. But when we began to delve deeply into how they manage their controls, and we had staff go up to HSBC and get the regular tour and all that, we had a whistleblower, we were surprised at what we consider was a lack of really tough controls that were absolutely managed and overseen by those at the very highest levels.

So what about that? And why do you think we have such a commitment if we have these banks that are still involved with money laundering and they get a slap on the wrist with some fines?

Mr. PONCY. That is such a fantastic question. I would spend the whole hearing on that if I could. It is an incredibly important one. I will try to be brief, starting with what we know.

One, the United States enforcement community is stronger than any community in the world by a long shot. Many of the banks, including HSBC, are foreign banks that operate within the United States.

Our law enforcement combined with our supervisors is frankly the only enforcement game in town, and this is in a global financial

system that we are connected to. So let's start with the recognition that despite the challenges that we face, we are operating in a global environment in which we are already putting tremendous pressure on institutions that operate here versus offshore. And we are competing with those same institutions.

Second, our law enforcement efforts have substantially changed the efforts of financial institutions that are operating in the United States. So when you look at these monitor shifts and you look at these injunctive actions and enforcement actions that the Manhattan district attorneys office, that the Southern District of New York, Eastern District of New York and others have taken, there is no doubt in my mind, I have been in these banks, that they are a different place than they were 5 years ago. And that is entirely owing to our enforcement commitment.

The question you raised, though, is important, and this is in my testimony. It is not clear whether the current enforcement environment that is so essential is going to be enough to change a global challenge of compliance, a culture of compliance that is questionable across not just the global banking industry, the global banking industry, these are our best, right? These are the ones who can block and tackle.

What about the non-banks? What about capital markets? What about money service businesses?

So it is just the beginning of the answer to your question, but it deserves more time.

Chairman FITZPATRICK. Thank you, Mr. Poncy.

The gentlelady's time has expired.

Mr. Pittenger, you are recognized for 5 minutes.

Mr. PITTENGER. Thank you, Mr. Chairman.

Mr. Poncy, in my discussions with the officials at FATF, I have raised the concerns about the compliance of the other 34 member countries with the 40 recommendations. And they come back to me and say the question asked by so many of these countries is the U.S. compliance, particularly as it relates to the beneficial ownership.

Would you speak to the importance of our compliance and how this affects our other member countries in causing them to be in greater compliance?

Mr. PONCY. Thank you, Congressman. That is a great question. The strength of our financial system, the integrity of it, rests upon our leadership globally. And the work that we have done in FATF and the credibility that we have achieved through our work at FATF and the work that we do back here at home is second to none.

But people are always looking at the United States naturally as a position of leadership and of vulnerability in an economy that we dominate as to how is the United States doing and is the United States practicing what it is preaching.

And when it comes to beneficial ownership, we have work to do.

I want to go back to, and this answers your question, Congressman Pittenger, some of what Congressman Fitzpatrick was asking about, customer due diligence versus what the Manhattan district attorney Cyrus Vance has mentioned about company formation re-

form. These are two ends that are both essential to achieve transparency on beneficial ownership.

They do it in different ways and they are not mutually exclusive; in fact, they are both absolutely necessary to comply with FATF and to achieve financial transparency.

On the one hand, anybody who wants access to financial services should be somebody that we know who they are. That is what customer due diligence is supposed to do. We need the Treasury rule out to meet FATF standards and have confidence that our banks and our financial institutions understand the people they do business with. That is one element.

The other element that the FATF is concerned with, with the United States, concerns company formation, which Mr. Vance has discussed. And to achieve compliance with that requirement requires us to reform company formation processes.

I know Mr. Vance's testimony and mine both recommend legislation to fix this. It will require legislation, and there are a number of ways to do it. But the point is that there are now solutions on the table that require action.

If we achieve compliance with beneficial ownership requirements, both with respect to customer due diligence and company formation, we will have addressed the overwhelming concern from FATF with U.S. compliance. And at that point, that strengthens our hand to continue to demand that other countries step forward on other matters.

Mr. PITTENGER. That is really the point I wanted to make. You emphasized the impact it has on our ability to lead and cause accountability from our other member countries.

Mr. PONCY. Exactly.

Mr. PITTENGER. Mr. Carlson, you referenced business email compromise. Have you seen evidence of the hacking of CFOs to exploit their system with wire transfers? Do you see this as a concern and possibility that terrorist organizations would deploy this type of method for financing their own operations?

Mr. CARLSON. I don't know to what extent it involves terrorist organizations, but we did issue last Friday a joint advisery with the FBI and the Secret Service on this new type of wire fraud, to try to alert the community that this is going on and to also provide some tips on how they can prevent it.

So we are seeing this where oftentimes a CEO or CFO is going on vacation, someone will get access to their email accounts, divert the email account, and then instruct the staff to transact a wire transfer. And it does require going through and developing some stronger controls around validating the request and confirming the request, particularly when you are talking about large dollar transactions and transfers that oftentimes are difficult to pull back or impossible to pull back, particularly if they are going overseas.

So we are seeing some evidence of that, but we are trying to be proactive and working in partnership with law enforcement to raise awareness and to provide guidance.

Mr. PITTENGER. Thank you.

Mr. Vance, regarding cyber, do we have the proper and necessary authorities in place to be able to bring justice to those who are in-

volved in the cyber war? And are those mechanisms in place to close out this behavior?

And if so, would Section 311 be a proper a method to use in that regard?

Mr. VANCE. Congressman, I first would say that it is the Federal Government that to date has been responding to foreign attacks on American institutions and companies. And so, I cannot speak for the Federal Government.

And quite honestly, Section 311 is not something that I am familiar with, and I don't want to answer a question that—

Mr. PITTENGER. I'm sorry. Maybe I should direct it to Mr. Poncy.

Chairman FITZPATRICK. The gentleman's time has expired.

Mr. PITTENGER. Thank you.

Chairman FITZPATRICK. So we will move to the ranking member of the task force, Mr. Lynch, for 5 minutes.

Mr. LYNCH. Thank you, Mr. Chairman.

Thank you all for your testimony. You have been very helpful.

Mr. Vance, the centrality of New York and Manhattan as a global financial center gives us some leverage and some ability to impact money flows to some of these terrorist organizations. So it gives us a little bit of leverage as well as the fact that the major reserve currency is the American dollar, the U.S. dollar.

So we are having negotiations right now with Iran, ongoing, about reducing the sanctions, and the negotiations have really centered around the nuclear development within Iran. And the sanctions seem to be being weighed as a consequence of eliminating the possibility of developing a nuclear weapon in Iran.

However, in practice, through Section 311 with the special measures there and 314, we have been able to use the legitimate banking system as a way to sanction Iran for funding terrorist activity. It is a totally different direction that they go in.

Actually, back in the day, I don't know if they still do it, Iran used to carry a line item in their budget for Hezbollah and Hamas, a direct line item for funding those terrorist organizations. I am not sure they still do that. I wouldn't be surprised.

So we have this difficult, this Gordian knot that we are trying to untie here, the idea that the Administration has said we will lower sanctions against Iran if they agree to cease and desist from developing a nuclear weapon.

However, the institutions that will benefit from the reduction in sanctions are the very same banks, Bank Melli and others and their central bank, that have been guilty of financing not only Hezbollah and Hamas, but also Al-Shabaab and Boko Haram and other groups throughout the Middle East, the Taliban more recently.

Is there a way—this is a tough question and you can all have a crack at it—to make that framework operate the way we wish? In other words, even though the Administration might say, okay, they have done away with their nuclear program and we feel we have verified that, I think there are a lot of banks out there that are going to keep those sanctions in place because they don't want to be tainted with the fact that they are now financing some of these terrorist organizations.

It is a dilemma that we are facing here. And while I would like to eliminate the nuclear threat, certainly there are a whole lot of other things in play here that I am not so comfortable with.

Please.

Mr. VANCE. Congressman, I would just say from my perch in Manhattan having done now eight of these cases involving foreign banks and terror funding and interruption of that financing, that much more than simply the dollar fines that have been taken as a result of the misconduct, but it has changed, I believe, significantly the attitude in foreign banking toward dealing with the American banking system, State and Federal.

So I think it has been, from my perspective, it has achieved what we wanted to achieve, which is honest banking as well as not having rogue regimes and countries being able to move money around the world, let alone through New York.

I have seen—even though I am a State and not a Federal person, and even though I am not an expert on foreign policy, I can draw a direct connection between the positions that we have taken in enforcement and the impact on a country like Iran which is a present and real danger, not just for the region, but for our country.

Mr. LYNCH. Mr. Poncy?

Mr. PONCY. Congressman, thank you. This is a hugely important question that is being debated now on the front pages for good reason.

There are three points I would make.

First, obviously if the Administration can secure a deal in which we eliminate the threat of nuclear proliferation from our greatest proliferation threat, Iran, that is something we should all support. The way that is done has to be very carefully crafted in a way that ensures that we have verification of the commitments that Iran can make, that Iran makes in that deal. And that is within the province of the Administration. And obviously, I wish them success in that.

But second, assuming that deal goes through and that it is verifiable, there is the question of how you unwind sanctions that have been imposed for a variety of derogatory behaviors, to your point.

And it will require very careful consideration not just by the Administration, but by banks to think about, what was the basis for the sanctions on Iran in the first place?

Long before proliferation, there was terrorism, to your point. They are still a state sponsor of terror. They are subjected to more terrorism financing and counter-terrorist financing controls than any other country around the world.

They are also subjected to intensive and preventive measures associated with money laundering and corruption.

These activities and human rights abuses and other bases for sanctions continue, regardless of whether or not there is an agreement on nuclear proliferation. That has to be a consideration in how sanctions are unwound.

And lastly, the AML obligations will continue to exist, even in the absence of sanctions, through which financial institutions should take very good care in how they deal with any Iranian financial institutions.

Chairman FITZPATRICK. Mr. Carlson, can you respond quickly?

Mr. CARLSON. I am not an expert on the AML rules. I do know that when we have these conflicts with countries like Iran, they do show up in my domain in terms of cyberattacks and responding to those issues.

So we are interconnected. Obviously, the financial services industry implements the rules that you put in place and that the Treasury Department puts in place.

I will say there is a growing concern within the industry around the compliance burden of a lot of these AML anti-terrorism laws. We at the same time are encouraging the Administration to do more, to create more of a deterrence against cyberattacks. And we know there is an Executive Order that was issued in April that basically leverages the AML and sanctions rule in order to do that.

We generally support it, but we have some concerns about the implementation and the additional burden it puts on the industry.

Mr. LYNCH. Thank you.

Chairman FITZPATRICK. I now recognize the gentleman from New York, Mr. King, for 5 minutes.

Mr. KING. Thank you, Mr. Chairman.

District Attorney Vance, actually all the members of the panel, but District Attorney, you supported in the last Congress the Incorporation Transparency and Law Enforcement Assistance Act which was introduced by Congresswoman Maloney. And I was a cosponsor. I believe Chairman Fitzpatrick was a cosponsor, and the ranking member of the full committee, Ms. Waters, was a cosponsor.

Basically, that would just require companies with fewer than 20 employees and/or less than $5 million in revenue to file information with Treasury disclosing beneficial ownership. And this is intended for the purpose of cracking down on shell companies.

Now, that and also the FinCEN rule have been opposed by the American Bankers Association. And I know Congresswoman Maloney's legislation, which I supported then and support now, has been looked upon as too much of a regulatory burden.

Can you address that and how much of a burden this is and how this would compare with other requirements that are imposed on the banking community?

Mr. VANCE. Let's just start, Congressman, with the issue of currency transaction reports. As in most cases, when there is a regulation that is going to be applied to an industry, industry usually, many industries, cry that the world is going to end and that it is going to be too expensive and it is going to drive businesses out of business or away from America.

We have learned how to live with currency transaction reports and it has been a powerful investigative tool in ordinary crime as well as terrorism.

Now, I understand that at least under one bill as drafted there would be an interim period where these rules would be applied to the States. There would be funding for the States in order to cover the costs of making this transition.

And so from my perspective, that all seems reasonable and appropriate and that the additional burden placed on a corporation by checking off one box and filling out a couple of names seems a small price to pay when the benefit is law enforcement, where nec-

essary, being able to investigate and prosecute crimes that are impacting not just our government, but our citizens, and many of those investigations relate to terrorism.

There are also—I understand people oppose it, but I also know that at least with regard to the Senate bill, there were many who supported it, including the Main Street Alliance, the American Sustainable Business Council, the National Money Transmitters Association, and on and on. There were many folks, including all of law enforcement, who supported that bill. So there is support and opposition, but I think the support is powerful.

Mr. KING. I know that the Federal Law Enforcement Officers Association, FLEOA, Fraternal Order of Police strongly supported it.

Mr. Poncy, can you comment on that?

Mr. PONCY. Thank you, Congressman.

I would just say that this happens often, but the proposed legislation that you are referring to was, in my view, terrific and would have gone a long way toward addressing the abuse of legal entities that we have seen and that Mr. Vance has outlined so eloquently.

The challenge in part is that you have two ways to get this beneficial ownership information, right? One is through company formation reform. And there are a lot of ways to do that, including the proposed legislation that you have cosponsored in the past.

Another is through requiring banks to obtain beneficial ownership information when customers seek access to the financial system.

Both of these requirements are necessary. These are not either/or.

So for example with the banks, the banks frankly on company formation, company formation reform is the bank's friend because there is no burden to the banks on that. That is a burden on States, on incorporation processes that will deliver the information that Mr. Vance is describing and should help banks because at that point there is more information for banks to then obtain from their customers.

Curiously, the banking industry has been somewhat absent from supporting the bill, but they don't directly oppose it because it is not their burden. It will ultimately accrue to their benefit.

And part of the reason why they may not be supportive is because if that goes through it will be easier for Treasury to get its rule out that requires banks to get that information when it is available, right?

So the two of these are related, but they are distinct and they are both essential. So I would simply recommend, and I have this in my testimony, that both ends of this become a priority to this committee.

One, let's table and adopt meaningful legislation to obtain beneficial ownership information that can be available to law enforcement in the company formation process.

There are a couple of different ways to do that. You are familiar with them. That needs to move forward. There is some burden associated with it, but it is nowhere near the benefit that reform would achieve not just for law enforcement, but frankly for our financial institutions that we are now hitting with enforcement action after enforcement action to manage risk.

And the second piece is to get Treasury to move on the customer due diligence rule with the support that it needs so that we require banks to obtain that information.

With those two elements in place, we comply with FATF standards, we increase our credibility globally, we manage risk to the financial system and we give law enforcement what it needs to pursue illicit financing networks.

Chairman FITZPATRICK. The gentleman's time has expired.

Mr. KING. Thank you, Mr. Chairman.

Chairman FITZPATRICK. We now recognize the gentleman from California, Mr. Sherman, for 5 minutes.

Mr. SHERMAN. This task force is focusing on terrorist financing that includes not only the non-state actors, but Syria, Iran, and certain other governments.

I would hope, Mr. Chairman, that we would get Administration witnesses here that can focus particularly on Iran, whether the 24 Iranian banks that have been sanctioned will continue to be sanctioned under this nuclear deal, whether the Iranian banks will continue to be denied access to the SWIFT system, and whether those banks found to be of money-laundering concern not because of the Iranian nuclear program, but for other reasons, will continue to be listed.

I would love to ask these witnesses, but asking them what the Administration will do may not be a good use of time.

But Mr. Vance, you identified that an Iranian bank, a sanctioned Iranian bank, ended up being the beneficial owner of certain property in New York. Have you seized that property?

Mr. VANCE. Actually, the Federal Government did. The Southern District of New York, which came along later and proceeded on the Federal asset forfeiture, and that occurred—

Mr. SHERMAN. If the Federal Government would stop objecting to the victims of Iranian terror suing the Iranian government, that could be used as a source to finance those victims.

Enforcement in this area requires prosecution. One thing that is related is a number of Swiss and other foreign banks have been hit with multi-hundred-million-dollar, in some cases billion-dollar, fines for conspiring with very wealthy Americans to allow those Americans to have secret bank accounts. Those secret bank accounts were for tax evasion, not avoidance.

So we get a chunk of money from the banks, we will get a chunk of money from the—I will call them taxpayers, but I guess I would call them non-taxpayers, these folks have also—and of course, we aren't prosecuting any of them, so we are not going to really effectively deter this in the future.

Those who cheat on their Federal taxes always do so on their State and City income tax returns as well.

Are you getting the information about those who have deliberately defrauded your State and City? And are you prosecuting them?

Mr. VANCE. Congressman, the answer is, to date, no. But in terms of what our current investigative posture is going forward, I think I can just indicate that is something we are looking at.

Mr. SHERMAN. The IRS has a policy of providing State tax collection agencies with information. And the too-big-to-jail should not

apply to those who, on their Federal and usually State tax returns, check a box saying, I have no foreign bank accounts, and in fact have foreign bank accounts so significant that we get a billion-dollar fine from the bank just for hosting that account.

Another area is we need the retailers to do a better job of holding onto the private information about credit cards. Does it make sense for us to impose liability on the retailer or to stick with the current system in which all the costs of these data breaches of credit card numbers are borne by the financial institutions?

Does any witness have a comment on that?

Mr. Carlson?

Mr. PONCY. Thank you, Congressman. Again, a hugely important question.

But in looking at the information sharing and liability issues, there is a tension, right? Because on the one hand, we want to make sure that institutions, whether retail or financial, that have sensitive personal information protect that information. That policy interest is well-established and obviously justifiable.

At the same time, liability for sharing that information is exactly what prevents us from putting together the information that we need to connect the dots.

Mr. SHERMAN. Yes, I am not saying that they should be liable for sharing the information with you. They should be liable for unintentionally sharing the information with criminal gangs based in Russia who are now selling my credit card information.

I want to sneak in one more question with Mr. Vance. But he may want to answer this for the record.

Perhaps you could give us a proposed statute requiring States to register beneficial ownership of closely held corporations keeping in mind that we may have to, for federalism reasons, exclude those corporations that have only beneficial owners within the borders of those States, but also letting us know whether this would really be useful or whether people would just form a Cayman Islands entity which would then be the sole and disclosed owner of the Delaware corporation.

Chairman FITZPATRICK. If the gentleman could answer quickly, or make a proposal to the committee in writing, whichever you prefer.

Mr. VANCE. Very good, thank you.

Chairman FITZPATRICK. Thank you.

The Chair now recognizes the gentleman from Florida, Mr. Ross, for 5 minutes.

Mr. ROSS. Thank you, Mr. Chairman.

Gentlemen, we know that Iran is a major exporter of terrorism and that their Islamic Revolutionary Guard has helped Hezbollah in training, not in cyber, but has helped in many ways.

Is there any known threat or at least perceived threat that Iran is in the process of training for cyber terrorism purposes?

Mr. PONCY. Congressman, I am not aware of any known, but it is clear as a state sponsor of terror, we, as you know, have grave concerns about the terrorism financing activity of Iran well beyond the nuclear proliferation concerns that are the subject of the deal.

Mr. ROSS. Correct. In fact, they have been described, Tehran has been described as being the central bank of terrorism. So is it more

likely than not that we would expect that not only the United States, but even our allies may be subject to cyber terrorism that has been brought about through Iran?

Mr. VANCE. I would say that it is greatly within the realm of possibility.

Mr. ROSS. Speaking with regard to what Mr. Sherman was talking about in terms of beneficial ownership information, there is a Federal issue, there is a reason that people incorporate in Delaware and it has to do with the State jurisdiction that they have.

The cumbersome way that we legislate here and the length that it takes, absent a crisis, we tend to just react at the time. And so, being able to promulgate legislation that would address the concerns in order to make sure that we have beneficial ownership information available for our law enforcement and others is monumental.

Is there any effort being made through the States so that we preserve at least their ability to control the incorporation process, but then to require that they also have information pertaining to beneficial ownership interests?

Mr. VANCE. Congressman, I am not aware, with the exception of two or three States, that there has been any interest in this beneficial ownership question at all. And I think the trend is very much in the opposite direction.

The reason we were so grateful that the Federal legislators were looking at this was because we believed that—

Mr. ROSS. I think it is absolutely important.

And I think, Mr. Poncy, you raised some good points in your testimony that this at least gives us the ability, while all of the other countries require this, but we don't. And I think we have to look at our States for that.

Also as an aside to that, the regulatory process, as much as I hate to see it used the way it has been used here for the last 6 years, might be the only avenue pursued in which we can require that this information be made available at least at the banking level. Wouldn't you agree?

Mr. PONCY. Absent regulation, it won't happen.

Mr. ROSS. Right.

Mr. Poncy, you have talked about our programs and AML and CTF and trying to get stronger, more enforcement because there is so much out there that we don't know.

What can be done specifically with some of our allies and making sure that these programs are done globally?

And specifically, if I could ask you to speak on our relationship with Turkey in regard to that.

Mr. PONCY. There is no question that we have a global challenge outside the United States in understanding and implementing what we call broadly targeted financial measures. That includes conduct-based sanctions on terrorism, proliferation, state-based sanctions against Iran, the Russian regime, and others, and regime-based programs.

Mr. ROSS. But we are being somewhat undermined, are we not, by some of our allies with these programs?

Mr. PONCY. The first point is that there is a global lack of capacity on this in general because of a lack of understanding that is owing to a lack of political will.

Mr. ROSS. Right.

Mr. PONCY. The second point is that within that lack of capability, there are different levels of challenges. One level is associated with our best partners, the EU, and legal restrictions that any time that you see a significant designation the EU is challenged for violation of human rights. And those challenges are winning, they are winning more often than not.

The viability of our sanctions programs and partners across the EU is in serious jeopardy. It has been for quite some time.

You take away the dollar clearing leverage in the United States and our sanctions programs wouldn't exist outside the United States. So that is challenge number one.

Challenge number two is in allies of ours that do not see politically sanctions the way that we see them. So the EU may see that politically, but is legally incapable of supporting it.

A country like Turkey doesn't politically agree with a lot of our sanction programs.

Mr. ROSS. Correct.

Mr. PONCY. And for those, those represent different vulnerabilities.

Mr. ROSS. And any suspension of sanctions for any reason is not going to lead to an opportunity to snap them back instantaneously because there is going to be a sense of dependency, a sense of investment of capital and resources that would prevent any snap back.

I see my time has expired.

Thank you.

Chairman FITZPATRICK. The Chair now recognizes the gentleman from Minnesota, Mr. Ellison, for 5 minutes.

Mr. ELLISON. Yes, I want to thank the chairman and ranking member and also our panel and my colleagues who have asked a lot of great questions today, and so good that they took some of the questions I was going to ask. But I do have some.

We have talked a lot about terrorism abroad, incredibly appropriate, but as the last few days have shown us, we have terrorism domestically, too.

And I guess my question is, can you share with us what sort of focus has been done to address these organizations? We are about to bury nine people in these coming few days, and while it is not clear whether or not this particular incident was the result of an orchestrated group, there is indication that he relied on services from a group.

And of course, we do know that in the case of several other attacks that they were affiliated. And these organizations do have money and resources and used them to do what they do.

Not only do we think about the horrible events at Mother Emanuel, but there were three people killed at a Jewish community center and assisted living facility in Kansas City not too long ago, and six people were murdered in a Sikh temple in Wisconsin.

The Southern Poverty Law Center publishes a hate map of internal hate groups that I think I have asked to be posted up there.

And some of these groups may be inciting violent action as we saw in South Carolina.

So my question to the panel is, how are financial institutions responding when some of these neo-Nazi groups, White nationalist groups, Klan groups, anti-government groups try to access the financial system? And do these financial institutions report such groups to regulatory agencies?

Mr. VANCE. Congressman, in New York City, in Manhattan, I have not experienced the problem you are talking about.

But if I can answer the bigger, broader question briefly, the terrorism threat has evolved to what is currently today a real risk of homegrown violent extremists operating in our communities.

What I think we can do is to make sure that there is the highest level of partnership between Federal investigators and, increasingly, local investigators.

We are blessed to have a New York City Police Department that created competency in counterterrorism under Ray Kelly, that has continued under Commissioner Bratton. But the reality is that the Federal Government cannot do it all. It needs more hands and eyes and ears on street corners in every city in America.

And our office has taken the challenge that we are going to find a way to support this counterterrorism mission by essentially developing leads, building cases independent of the Federal Government having to come up with those leads. And then the Federal Government can screen them and we can decide whether the case is a Federal case or a State case.

But in the evolving threat, I believe that we need to see increased leadership from the Federal Government to bring into their anti-terrorism efforts the work not just of local police departments, but of prosecutors. Prosecutors around the country at the State level would be very happy to help in this regard. But many do not know where to begin.

Mr. ELLISON. Mr. Poncy, is this on our radar screen? We are very appropriately focused on some of these foreign terrorists and groups that even come here and commit acts of terror for various motivations. But some of these historic groups are still a problem. Are we tracking them financially?

Mr. PONCY. Thank you, Congressman. First, let me just say that I, in the strongest possible terms, support everything Mr. Vance has said.

I do think, when you look at historically what we have done since 9/11, the focus is clearly on foreign terrorist organizations. Our immediate focus after 9/11 was on what infiltration those organizations may have in our local communities. And so, we took immediate action, as you may recall, against a number of—

Mr. ELLISON. Mr. Poncy, Mr. Poncy, I definitely think what you are saying is incredibly important. But one part, in these last 9 seconds, is that we do think about the 9/11 and the aftermath and we are right to do so. But are we having a broad approach to all the terrorist threats and not just the Islamic ones? Although I want you to go after them, too, I also want you to go after these other groups. And are we doing that financially?

Mr. PONCY. I think we are trying. The challenge is that our effort is aimed at organizational capacity, right? So rogue terrorists, the

only way to stop that is through what Mr. Vance has said. And it doesn't mean that we shouldn't act and it doesn't mean financial institutions don't have a role.

It is just to say that our ability to stop rogue terrorist acts, even inspired acts, as Mr. Vance has said, homegrown violent extremism of any stripe, really requires partnership at a local level. There is no substitute for that.

Chairman FITZPATRICK. The gentleman's time has expired.

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

Mr. BARR. Thank you, Mr. Chairman.

And Mr. Poncy, a question to you about the Society for Worldwide Interbank Financial Telecommunications or the SWIFT system, which as you know enables the transfer of trillions of dollars globally on an annual basis. It helps international transfers flow smoothly.

As part of the U.S.-led sanctions against Iran, and pursuant to a law approved by the European Union in March of 2012, the SWIFT system disconnected all Iranian banks targeted by the United States and our European allies. These banks were targeted for their role in enabling Tehran to avoid sanctions and engage in illicit activities such as transferring funds and materiel to their proxies, Hezbollah and the like.

My understanding is, in the course of these negotiations with Iran, one of the very first concessions in terms of the sanctions relief that Iran is seeking is reconnecting Iranian banks to the SWIFT system.

So my question is, do you think that SWIFT access is useful leverage in terms of imposing sanctions? And how significantly has the disconnection to the SWIFT system impacted the Iranian banking sector?

Mr. PONCY. Great questions. And there can be no doubt that was a monumental movement in what was a series of movements in a campaign to intensify financial pressure on the Iranian regime. That was a signature moment and it required the full support of our European colleagues to take that action.

What led to that support was ongoing concern over the proliferation of nuclear technology and the building of a missile development program and nuclear technology in Tehran.

The challenge that we are now facing, in many respects, is aside from the negotiations that are happening, about which I have an opinion, but it is not an expert one by any view, but obviously we should all hope that we can achieve an outcome where proliferation is no longer a threat.

If that happens, two things are going to happen. One is the ongoing concerns that Iran presents to us, the threats that have led to over 40 years of sanctions, including, for the most part, for activities above and beyond proliferation financing, there has been no discussion of that activity because that is not what is in the confines of the deal.

It is within the confines of the risks that our financial institutions need to worry about. It is also within the confines of sanctions programs that we have on the books.

It is not within the confines of the pressure that led to the de-SWIFT'ing, so to speak, of Iranian banks.

So if I were to prognosticate, if a deal moves forward in which commitments from Iran are credible on nuclear proliferation, the SWIFT program will go back into place. That does not mean that our sanctions necessarily are pulled back on nonproliferation activity and it certainly doesn't mean that our financial institutions shouldn't be watching, managing, monitoring, and preventing illicit financing transactions associated with any engagement with Iranian financial institutions.

Mr. BARR. Let me ask you this question. Would reconnecting Iranian banks to the SWIFT system, in your judgment, lead to significantly increased risk that financing would flow to Hezbollah, Hamas, some of these proxies that Iran has allied itself with?

Mr. PONCY. Unless there are controls associated with how they are plugged back in, unless there are controls associated with how they engage with our financial institutions, I would continue to worry about those risks.

Mr. BARR. Let me shift gears a little bit to the Obama Administration's announcement on a change to hostage policy. And while not directly related to the financial system, it could have an impact on the financial system in terms of family members now being allowed to negotiate with loved ones' captors and accessing the financial system in order to transmit ransom.

At first glance, the policy would appear to raise incentives for terrorist organizations to take Americans hostage. And also, what impact would this potentially have on the financial system? Any opinions about the policy and the risks that it may pose?

Mr. PONCY. Thank you, Congressman. I had a few moments with Congressman Pittenger on this. And this is the worst dilemma imaginable, right, where you have to decide whether or not you allow families whose loved ones are kidnapped, and frankly with the beheadings we have seen I think any of us would do whatever we could in our power to save our loved ones. Asking the government to step in and aggressively enforce a policy against that is difficult.

On the other hand, we all know that kidnapping for ransom is an increasing part of how these terrorist organizations finance their operations. It is a hellish dilemma.

What I would argue, because I am not in a position to judge frankly what our policy is on this, is that understanding that kidnapping for ransom (KRF) is on the rise, understanding that puts us in an incredibly difficult position, that we need to go to our allies and say we understand why this is a difficult dilemma, we also know that state-sponsored, effectively allowance and support of ransom payments that facilitate KFR contribute to the problem, why don't we develop a strategy for how to deal with territories that are under the control of terrorist organizations or where terrorist organizations operate that we know create risks of KFR.

It is no secret that if you go into ISIS-controlled territory, KFR risks go up. It is no secret that if you are operating in areas controlled by Boko Haram, KFR goes up. These are well-known, established facts.

The real question is, what are we doing to deliver necessary relief and assistance to these areas in ways that allow our NGOs in to service needs that we recognize, in ways that protect them and others from this sort of activity?

I don't know that we have done enough thinking about that as a global community. And I do know that is something that the Financial Action Task Force members are looking at. How do we deal with terrorism financing associated with territory that is under the control of terrorist organizations? It is the biggest dilemma we face.

Chairman FITZPATRICK. The gentleman's time has expired.

Mr. Rothfus of Pennsylvania is recognized for 5 minutes.

Mr. ROTHFUS. Thank you, Mr. Chairman.

Mr. Poncy, what can the U.S. Government do to improve the implementation of effective AML/CFT programs among financial institutions with foreign correspondent banking relationships?

Mr. PONCY. That is hugely important. I am sure Mr. Vance could tell you that every enforcement case that I can think of that has grabbed the headlines in recent years has been one in which foreign correspondent relationships are key. And that happens for a couple of reasons that I tried to allude to earlier in my remarks.

One is that our enforcement environment is so far above any other enforcement environment in the financial system that when financial institutions seek to clear dollars, and they must move through New York or through the U.S. financial system to do that, as a general matter, they encounter a different level of compliance concerns associated with the enforcement actions we have taken.

What that means is that the correspondent relationships that are essential to clearing dollars become the pathway that exposes our financial system to all forms of illicit finance.

And the enforcement actions that we have seen repeatedly bear that out, whether it is for violation of sanctions programs and stripping activity, whether it is for violation of AML controls and the taking of drug money through cash without appropriate customer due diligence, it is through our correspondent relationships that this dirty money enters our system. So it is critical to protecting our financial integrity.

This Congress did an incredible job post 9/11, the Congress in general, in giving us authority as a government, giving the government authority under Section 312 of the Patriot Act to strengthen corresponding controls. And I would say that as a general matter, we have done a pretty good job at that.

At the same time, I would say that the complexity of flows that are moving through those correspondent relationships bears stronger compliance programs. And that is exactly what many of the enforcement actions that have been taken to date have insisted on, is looking at stronger programs to monitor and manage risks associated with clearing dollars and any other form of correspondent activity that is flowing through our banks.

Where this game is headed and where I think concerns need to be focused is in the non-banking space. What happens with respect to correspondent relationships between non-bank financial institutions? How are those being managed? And what kind of risks are we seeing?

Mr. ROTHFUS. Yes. I want to raise this. On June 12, 2015, The New York Times published an article that described how tough it is to impose and administer economic sanctions in an effective and meaningful way. It identified individuals and organizations that are crowdfunding the separatist conflict in eastern Ukraine.

Individuals who are designated by both the United States and European Union for economic restrictions are freely raising donations, channeling funds to Sberbank, a prohibited state bank in Russia, to buy equipment and stand up modern combat-ready military units fighting the Ukrainian central government.

Because correspondent transactions are permitted with otherwise restricted banks, Visa, PayPal and Western Union, the article claims, have all facilitated the crowdfunding.

How can government agencies here and in Europe effectively impose economic sanctions when targeted entities can evade the effort?

Mr. PONCY. The activity you are referring to, Congressman, I am not familiar with the specifics, but I can tell you that Sberbank, because it is subjected to a different kind of sanctions program, it is an SSI-designated entity. What that means is that there are sanctions against Sberbank with respect to debt and equity instruments that are used to benefit Sberbank.

But those sanctions are calibrated to put financial pressure on the Russian regime in a way that changes their behavior in the Ukraine. But they are not designed to cut Sberbank off from the financial system. And there are a lot of reasons for that.

But it does complicate efforts to then address what might be activity that offends or sanctions against Russia and parts of Ukraine for the activity that is going on there if that activity is not part of a specific targeted financial sanction program.

And the Sberbank designation is really not a designation against Sberbank as much as it is against a Russian regime that we are trying to, through financial pressure, change its behavior.

So it continues to represent a gateway that is permissible under the current sanctions programs and frankly is necessary to maintain what are complicated capital market flows between Eastern Europe and Russia on the one hand and the U.S. market.

If those flows are squeezed through additional sanctions, that may have collateral consequences beyond that of what you are describing.

I know the Administration has historically looked at this very closely. It is a very complicated set of measures. But I will say that the advent of this program, the SSI program, is exactly where sanctions needs to go, to target specific types of activity in addition to general actors that enter our financial system.

Mr. ROTHFUS. If I could jump in really quick, going back to this issue of beneficial ownership and disclosure, are there any legitimate business reasons for an entity not to want to have its beneficial owner's identity made public?

If Mr. Vance, and maybe Mr. Poncy could comment on that?

Mr. VANCE. Yes. I think there are understandable and legitimate reasons. It may be, for example, that someone, an individual is a well-known individual and does not want his or her identity made

public and, therefore, a target of harassment or cyber bullying there. And the same would apply for businesses.

But the fact that there is a legitimate reason to want to remain anonymous does not mean, in my opinion, that there should not be an availability of the Federal Government, or State government to get this information by subpoena and have the other information remain in confidence at the State and not disclosed publicly.

Chairman FITZPATRICK. The gentleman's time has expired.

Mr. Schweikert of Arizona is recognized for 5 minutes.

Mr. SCHWEIKERT. Thank you, Mr. Chairman.

Can I ask us all to sort of take a step backwards and say, what if I had this amazing ability to see money that is moving to all types of bad actors, whether it be money flowing from drug cartels, terrorist financing, bad actors out of Russia or wherever we may deem it, what would that money look like?

My fear is that much of the conversation we have had in here is money moving through fairly formal channels. How much of that bad-actor money, let's just call it that to make up a title, is moving in commodities?

It was a decade or two ago we used to hear the stories of diamond exchanges that were just a way of moving value. Informal networks of deposit here and somehow it pops up in the rural areas in Pakistan.

And I would like to start with Mr. Vance. Are we making a mistake in believing that a sanctions regime, a regulatory regime, an ID'ing, an intelligence regime that focuses on formal networks doesn't just move the money to informal?

Mr. VANCE. I think we are not fully attacking the problem if we are only looking at financial institutions as the group whose behavior we are trying to change.

In our jurisdiction in Manhattan, we have a number of investigations moving money in the manner you describe, informal bases, not through official, organized entities that we believe are going to fund terrorist activities elsewhere in the country.

We have a number of them in ongoing investigations, and so I can't quantify that, Congressman, in terms of how big that number is in either New York City or the country. But I think it is something, again, that every, that large metropolitan prosecutors should be looking at to support the efforts that are being done by Federal prosecutors.

Mr. SCHWEIKERT. I want to do a hop and then back one.

Mr. Carlson, one of my fears here is we come up with both legislation in support for the Administration, we squeeze down and we make a more robust system of bad actors moving cash that is right under our nose that we cannot smell. Mixed metaphors.

You have done compliance with, what, large institutions in the past. When you started to clamp down, did that money just stop or did you see it moving to other types of activities?

Mr. CARLSON. I don't have any personal experience to comment on that. I do know at least from where I sit that what we certainly need is better mechanisms to share information around these bad actors and how they are affecting institutions' critical infrastructure, other parties.

Because right now we are in the world of playing constant defense in a constant flow of attacks, and so we feel like we are fighting this a little bit with our hands tied behind our backs in terms of not having all the tools that we could have to at least share the information so that we can take appropriate steps to respond.

I think in response to some other questions that were raised, we certainly need a greater role for deterrence, and that includes obviously enforcement in terms of what you require reputable businesses to do to enforce it.

But that is where I think the Congress needs to provide resources to law enforcement to go after these parties and to prosecute and not always go after the institutions that are implementing policy.

Mr. SCHWEIKERT. But my fear is, do we end up enforcing and create a more robust mechanism that just goes right around our back door?

Mr. Poncy?

Mr. PONCY. It is a great question. I will make four quick points. The first is the game of illicit finance is a cops-and-robbers game that will never end, right? So in many respects, what we are chasing will always be there, it is a question of where it is and how disruptive we can be.

Our objectives, in this campaign, as long as there are bad guys in the world, there will be bad-guy financing. Our objectives are to make it costlier, riskier, and more difficult for these guys to operate, get the money they need, move it from place one to place two. That is our objective.

In that respect, moving people out of the formal banking system to make it harder for them to deal with value transfer is a sign of success, but it is not the end of the road.

Mr. SCHWEIKERT. But in a world of technology where this is now my bank, it is cracking down on the institutions.

I constantly wonder, and I know I am almost out of time, whether much of this resource we should be really doubling down on the financiers, the people who use their wealth and treasure for bad acts, and the receivers of that.

So possible success on the barbells and not necessarily those who are in the middle of the transfer.

Thank you. I yield back, Mr. Chairman.

Chairman FITZPATRICK. The gentleman's time has expired.

The gentleman from Texas, Mr. Williams, is recognized for 5 minutes.

Mr. WILLIAMS. Thank you, Mr. Chairman.

Mr. Vance, you mentioned specifically that your office has supported the Incorporation Transparency and Law Enforcement Assistance Act previously.

As a former secretary of state myself, of Texas, our association has previously opposed this legislation due to concerns over implementation costs. In fact, State secretaries have advocated for the collection of ownership entity information by the best paper trail that already exists for Federal tax filings and customer due diligence requirements for the U.S. financial institutions at no additional cost to taxpayers or businesses.

So in addition, this proposal expands regulatory authority into an area that has traditionally been the jurisdiction of the States.

I would like to hear your comments on the concerns we hear from the association.

Mr. VANCE. I understand, Congressman, that there are questions of cost and that there will be some additional costs in various States for implementation of the beneficial ownership rule.

What I would respond to is I think we have to measure the benefits versus the detriments. I personally, having listened to the arguments of those who oppose this legislation, I am more persuaded that the benefit of enabling our law enforcement officials to identify illegal money movement is outweighed by the incremental additional costs.

I respect the fact that will occur, but that occurs, I think, in any regulatory scheme that is imposed upon the States.

Mr. WILLIAMS. Return on investment.

Mr. VANCE. Yes. I think you will get good return on investment criminally, in terms of criminal prosecution.

Mr. WILLIAMS. Next question also to you, Mr. Vance. Based on your experience as a prosecutor, what are the challenges associated with prosecuting terrorist financing-related cases?

Mr. VANCE. I am speaking from a State perspective. We are not like a typical State prosecutor's office because we do a lot of this work and most don't. But I still am not the Federal Government.

So one problem from where I sit is the ability to trace money once it gets to Lebanon or some other jurisdiction where we no longer have eyes and ears on the ground.

We have been involved in a number of cases where we believe we know what is going on, we can trace the money from wherever it is in the United States or even in South America to a Middle Eastern country typically, but then we lose the trail.

So how do we develop information and allies in those jurisdictions, which is a tough thing, to enable us to make those cases?

I think that is the biggest problem. And this is particularly, this is money going out to those jurisdictions, we are not talking about large financial institutions clearing dollars to us.

Mr. WILLIAMS. Let me give you a follow-up question. To what extent do U.S. law enforcement investigations and subsequent prosecutions strategically prioritize cases involving the most pressing terrorist financing threats?

Mr. VANCE. I cannot speak to the Federal Government's prioritization, which I think raises the question of, should there not be more coordination between Federal prosecutors and regulators on discussion of these priorities with State law enforcement who could in fact initiate or help in achieving those priorities?

So I am not privy to what the U.S. Government, what their list of priorities are. But if I knew them and if I was told how we could help in achieving them, that is what I would do.

Mr. WILLIAMS. Okay, thank you.

And I appreciate all of your testimony.

Mr. Chairman, I yield back.

Chairman FITZPATRICK. The gentleman yields back.

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

Mr. HILL. Thank you, Mr. Chairman.

And I thank the ranking member.

I also want to thank Mr. Lynch and Mr. Sherman for their pointed and excellent questions on Iran and Iran financing and I think the fallacy of the deal as we come up on the June 30th negotiation deadline.

Mr. Vance, I thought Mr. Williams did a good job of talking a little bit about the Secretaries of State and the burdens there. I understand those, some States are better than others.

I am going to ask this question as a former Deputy Assistant Secretary of Treasury and a banker of 35 years. So on the credit side of all banks, people get beneficial information. And if we were asked by a law enforcement officer, we would certainly provide that.

So I think the real challenge then becomes on the deposit side under Gramm-Leach-Bliley. We do know our customers, we do identify them, we do have two forms of ID. But in a business we also verify the business exists through the Secretary of State function, but we don't always know beneficial owner on the depository side.

One of the primary ways of finding depository ownership is through the tax system. Just about 6 years ago, we had a complete, wholesale redo of the Form 990 for private charity entities, which was very painful to implement.

But we have LLCs and pass-through ownership and, by definition, beneficial ownership is contained in that tax return and public companies are, of course, public. So we are really talking about C corps, I guess, for IRS purposes.

Could you reflect, as you did for Mr. Williams, on Secretaries of State, and talk about the use of existing IRS forms for determining and obtaining that information?

Mr. VANCE. Congressman, as I indicated earlier in a response, our State government access to those records is limited. And therefore, I really can't—

Mr. HILL. From one State to the other as a district attorney?

Mr. VANCE. —from the Federal Government to the State. And so therefore, we would appreciate it if there were changes in Federal legislation that permitted the IRS to provide information directly to a local prosecutor's office upon a certain showing.

That doesn't really exist now, and so therefore I can't comment further intelligently other than to say that access to Federal tax information, individual and otherwise, is not generally something that we at the state level get access to.

Mr. HILL. But when you get access to it, you acknowledge that is where beneficial ownership lies.

Mr. VANCE. I think there will be information relevant to beneficial ownership. But I am still, respecting that others disagree, I am having a hard time just personally understanding that the net negative of understanding when a corporation is formulated who is the owner of it and identification for that individual.

I don't necessarily think that is an inhibition to commerce, to business development. And so from my perspective, I don't look at that as an impediment that outweighs the benefits to public safety on the other side.

Mr. HILL. But you would support some sort of beneficial ownership form for a C corp filing, for a private company's C corp filing?

Mr. VANCE. I will say I think I am going to have to understand more closely what the issues would be for a C corp. I don't pretend to understand the specifics.

But where one would want to be is, with any filing of any corporation in a State, is to understand who the owner is and to prove that person is in fact the owner.

Mr. HILL. Mr. Poncy, on this FinCEN Treasury proposal, it suggests that beneficial owners, anyone who owns more than 25 percent of the equity interest in a company, and as somebody who has been doing this for 35 years, if I were hiding my interest, I wouldn't own 25 percent, I would own 1 percent and 99 percent would be divided by as many people as possible.

So I find I am not even sure as drafted it is particularly helpful to your mission. Do you want to comment on that?

Mr. PONCY. Absolutely. Thank you, Congressman. There have been experts from both the financial system and from the counter-illicit-finance community for decades who have looked at this question of beneficial ownership in the context of the Financial Action Task Force, from financial centers around the world.

It is a difficult problem. You can't draw a line and say this fixes it; I fully agree with you.

At the same time, it is clear that if we were to obtain beneficial ownership information as defined in the proposal, which is not just 25 percent ownership, because you are right, that just invites structuring, I will say that means you have to find five guys now who are willing to front for an organization rather than one.

And that is not the only element of the definition. There is also an element of control. And if you think about what that means, it means that if there are meaningful consequences to not presenting information, law enforcement no longer has to prove money laundering, they have to prove that you committed fraud in representing who you represent.

That is an easier case, it is a bigger lift. And those guys talk about whose interests they represent when they have to go to jail for not disclosing that truth.

Mr. HILL. Thank you, Mr. Chairman.

Chairman FITZPATRICK. The gentleman's time has expired.

The gentleman from Maine, Mr. Poliquin, is recognized for 5 minutes.

Mr. POLIQUIN. Thank you, Mr. Chairman. I appreciate the time.

And thank you, gentlemen, for being here. I appreciate it.

You folks have an awful lot of experience on the ground dealing with these issues. And it is so important that you help educate us here in Congress in making sure that our country stays on offense against these threats to our homeland and our freedoms.

I hear on an ongoing basis the issue with regulation throughout our economy, in the financial services sector and elsewhere. Some of the numbers I looked at, gentlemen, and I am sure you have seen them, too, is that the annual cost of regulations, to comply with regulations, to our business community is something like $1.7 trillion per year. That is about 1/10 of our GDP output every year. And that is a huge cost, waste of time and so forth and so on.

Now, at the same time, I know there has to be a balance between making sure there is proper regulation that the businesses can handle and pay for and in keeping us safe.

Our economy has been, notwithstanding the problems we have now, the envy of the world for a very long period of time. It has given us the opportunity to have better lives, fatter paychecks, through more freedom. And the reason we have this strong economy that has lasted for so long, notwithstanding its problems, is because we have such a deep, diverse, and creative financial sector.

Without this financial sector being healthy and growing, we do not have the economy we need to have; and therefore, we will not generate the tax revenues we need to protect ourselves.

So this is absolutely critical. And I know we are all onboard here.

We had a fellow who came into our office not long ago who is a senior manager at a financial services company. And he was going on about how many different regulators that he has to deal with when it comes to an examination dealing with cybersecurity. He deals with the Federal Reserve, the SEC, the Comptroller of the Currency, maybe FSOC, and also the FDIC.

And I know this has been discussed earlier, gentlemen, and I am thrilled to death to hear that with all these problems that we have, it seems like we are all in agreement, is that why in the world can't we coordinate this examination process to keep our financial services sector safe, as best we can keep money out of the hands of terrorist organizations, but not put these poor folks out of business?

Now, you folks have the experience with this, I don't.

So Mr. Carlson, we will start with you, if you don't mind, sir. Do these various regulators of the financial sector have the personnel and the talent to make sure they can do their work when it comes to investigating cyber activity? And what is the best way to coordinate this activity among these institutions?

Mr. CARLSON. I think it is a qualified "yes" in that the agencies do have expertise to conduct cyber exams.

I think an area we have been advocating that they do more on is to try to harmonize the requirements both at the policy level and at the examination level across all these different U.S.-based regulatory agencies.

We have also advocated that they work with their counterparts overseas to also harmonize, given that many of the larger firms are global firms and have to deal with requirements in the EU and Asia as well.

It is a huge issue in terms of cost and compliance. But they do have the capability.

They are also struggling with some of the same issues we are struggling with in our sector, as is the government, and that is talent in the information technology field. There is a limited supply of talent and everyone is vying for those people.

Mr. POLIQUIN. Mr. Carlson, is the information that is required from these regulators uniform enough? Is there enough overlap such that there might be uniformity when it comes to the type of information that is asked, the reporting requirements, how it is reported and so forth and so on? Because some of these folks come

to our office and they say it is different for everybody, even though they are generally asking for the same information.

Is that too simplistic or can that be streamlined?

Mr. CARLSON. It can be streamlined further. There are efforts already in place through what is called the Federal Financial Institutions Examination Council (FFIEC), which includes the Federal Reserve, the FDIC, the OCC, and the CFPB; they all coordinate together in terms of developing unified procedures.

Mr. POLIQUIN. And do I hear you saying that there is one entity, separate from all these other institutions we have talked about, that coordinates this activity?

Mr. CARLSON. It is a body that then coordinates with all of the other bodies.

Mr. POLIQUIN. And in your opinion, are they effective? And do they have the support they need from Congress to make sure they are effective?

Mr. CARLSON. They are effective. Could they do a better job? Yes.

Mr. POLIQUIN. And how could they do a better job, Mr. Carlson?

Mr. CARLSON. More intensive collaboration, more engagement with the sector in terms of new requirements, as well as constantly revisiting existing requirements to make sure they are relevant.

Mr. POLIQUIN. Okay. So this is not a resource issue, this is not a money issue, it is just providing some leadership—

Mr. CARLSON. Both.

Mr. POLIQUIN. —making sure someone steps up and gets this done.

Mr. CARLSON. It is both. It is a resource issue, but it is also a leadership coordination effort.

Mr. POLIQUIN. Do you think there is enough intense focus and priority from the administrative branch to make sure this happens, the Executive Branch?

Mr. CARLSON. There is an unprecedented level of engagement in the broader Administration on cybersecurity issues, from the White House to a multitude of agencies, from the Treasury Department, regulators, Homeland Security, law enforcement, intelligence communities. We are in a completely different world over the past 3 years in terms of the level of engagement with multiple government agencies.

Mr. POLIQUIN. And do you think, is there anything that we can do in this committee or Congress can do to help with that process?

Mr. CARLSON. I think, number one, it would be immensely helpful to pass cyber-threat information-sharing legislation.

Number two, it would be important to make sure that agencies are properly funded so they can fulfill their missions, whether it is law enforcement or even the regulatory agencies.

And three, I think there is an importance in investing in R&D. It is an area where the government has really stepped back on kind of core R&D, particularly around technology and infrastructure and things of that nature.

Mr. POLIQUIN. Gentlemen, thank you very much for being here. I appreciate it. Let's make sure we solve this problem. Thank you.

I yield back my time.

Thank you, Mr. Chairman.

Chairman FITZPATRICK. The gentleman's time has expired.

The Members' questions are concluded.

Again, I would like to thank our witnesses for their testimony to the task force today.

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.

And without objection, this hearing is adjourned.

[Whereupon, at 4:24 p.m., the hearing was adjourned.]

A P P E N D I X

June 24, 2015

Testimony of John W. Carlson on behalf of the

The Financial Services Information Sharing & Analysis Center (FS-ISAC)

Before the U.S. House of Representatives Committee on Financial Services

June 24, 2015

Chairman Fitzpatrick, Vice Chairman Pittenger, Ranking Member Lynch, and members of the Task Force to Investigate Terrorism Financing, thank you for inviting me to testify at this hearing, "Evaluating the Security of the U.S. Financial Sector." My name is John Carlson, and I am the Chief of Staff of the Financial Services Information Sharing and Analysis Center (FS-ISAC). I am testifying on behalf of Bill Nelson, President and CEO of the FS-ISAC, my FS-ISAC colleagues and our membership.

You asked me to discuss "the security of the U.S. financial sector." My testimony provides: a) an overview of the FS-ISAC, including our role in information sharing and collaboration; b) an overview of the security threats facing financial institutions; an overview of key regulatory requirements and the strong risk management culture in the financial services sector; and c) suggestions for actions the Congress could take to improve information sharing and enhance the security of the U.S. financial sector.

FS-ISAC BACKGROUND

The FS-ISAC was formed in 1999 in response to Presidential Decision Directive 63 (PDD 63) of 1998, which called for the public and private sectors to work together to address cyber threats to the nation's critical infrastructures. After the 9/11/2001 attacks and in response to

Homeland Security Presidential Directive 7 (and its 2013 successor, Presidential Policy Directive 21) and the Homeland Security Act, the FS-ISAC expanded its role to encompass physical threats to the sector. The FS-ISAC is a 501(c)6 nonprofit organization and is funded entirely by its member firms and sponsors.

The FS-ISAC's mission is to help assure the resilience and continuity of the global financial services infrastructure and individual firms against acts that could significantly impact the sector's ability to provide services critical to the orderly function of the global economy. The FS-ISAC's goals are to disseminate and foster the sharing of relevant and actionable information and analysis among participants to ensure the continued public confidence in the global financial services and to protect the financial services sector against cyber and physical threats, vulnerabilities, and risk. We act as a trusted third party that facilitates sharing of actionable threat, vulnerability and incident information (both attributed and non-attributed) and trusted manner among members, the sector, and its industry and government partners, ultimately benefiting the nation.

The FS-ISAC has grown rapidly in recent years. In 2004, there were only 68 members which were mostly large financial services firms. Today, we have about 6,000 member organizations, including commercial banks and credit unions of all sizes, markets and equities firms, brokerage firms, insurance companies, payments processors, and 40 trade associations representing all of the U.S. financial services sector. Because today's cyber criminal activities transcend country borders, the FS-ISAC has expanded globally and has active members in over 35 countries.

Since its founding, the FS-ISAC's operations and culture of trusted collaboration have evolved into a successful model for how other industry sectors are organizing themselves around this security imperative. FS-ISAC information sharing activities include:

- Delivery of timely, relevant and actionable cyber and physical email alerts from various sources distributed through the FS-ISAC Security Operations Center (SOC);
    - The appendix includes samples of our communications to members that convey, among other things, the type of alert, criticality level, and how the information should be handled, leveraging our "traffic light protocol"(TLP).
- An anonymous online submission capability to facilitate member sharing of threat, vulnerability, incident information and best practices in a non-attributable and trusted manner;
- Support for attributable threat information exchange by various communities of interest and circles of trust representing chief information security officers and business continuity executives, payments processors, and clearing houses.
- Regular threat information sharing calls for members and invited security/risk experts to discuss the latest threats, vulnerabilities, and incidents affecting critical sectors;
- Rapid response briefings to members when a broad-scale threat or attack is imminent or underway;
- Emergency threat or incident notifications to all members using the Critical Infrastructure Notification System (CINS); and

- Participation in various cyber exercises such as those conducted by DHS (Cyber Storm I, II, and III) and support for cybersecurity exercises such as the Hamilton series, CyberFIRE, and Quantum Dawn as well as member-led exercises such as the Cyber Attack against Payment Processes (CAPP) simulation exercises that the FS-ISAC sponsors.

Working with our members and other organizations, the FS-ISAC is engaged in numerous initiatives to:

- Improve information sharing content and procedures between government and the sector;
- Help automate, distill, prioritize and make cyber threat intelligence actionable for our members;
- Conduct joint exercises to test our communications, response and resiliency protocols during incident scenarios affecting different segments of the financial system;
- Maintain an "All Hazards Crisis Response Playbook" and within it a "Cyber Response Coordination Guide" that leads incident responders and executive decision makers through decision and action processes based on identified impacts and severity of incidents;
- Develop industry best practices and resources that can be used effectively by smaller financial firms with limited cyber capabilities;

- Engage with other critical sectors (e.g., communications, energy, information technology) and international partners to understand and leverage our interdependencies;
- Encourage broader use of the voluntary National Institute of Standards and Technology (NIST) Cybersecurity Framework, including among small and mid-sized financial institutions across the country; and
- Develop best practices guidance for operational risk issues involving third party risk, supply chain, and cyber insurance strategies.

FINANCIAL SECTOR PARTNERSHIPS

In addition to supporting individual financial institutions, the FS-ISAC works closely with the Financial Services Sector Coordinating Council (FSSCC) and with numerous national and state-based financial associations, including the American Bankers Association (ABA), BITS/Financial Services Roundtable, Credit Union National Association (CUNA), Independent Community Bankers Association (ICBA), Securities Industry & Financial Markets Association (SIFMA), and state banking associations.

The FS-ISAC collaborates with other sectors, including energy/electric, telecommunications, merchants/retailers, real estate and others. The FS-ISAC coordinates with other information sharing organizations and currently serves as the chair of the National Council of ISACs (NCI). The FS-ISAC coordinates and collaborates with numerous government agencies, including: the U.S. Department of Treasury, U.S. Department of Homeland Security (DHS), regulatory agencies that are part of the Federal Financial Institutions Examination Council (FFIEC), U.S.

Secret Service (USSS), Federal Bureau of Investigation (FBI), the intelligence community, and state and local governments.

As one example of our partnerships, we announced in early May a strategic agreement with the newly created Retail Cyber Information Sharing Center (R-CISC). Through the agreement, FS-ISAC is providing key advisory services and best practices, operational support and technology capabilities to help R-CISC deliver on its core mission to provide threat information sharing and cyber security for retailers.

In addition, the FS-ISAC worked with R-CISC and the U.S. Secret Service in November 2014, on a joint advisory on "protecting merchant point of sale systems during the holiday season." The advisory recommended possible mitigations for common cyber exploitation tactics, techniques and procedures (TTPs) based on previous attacks. The FS-ISAC continues to work with U.S. Secret Service and the R-CISC and is currently working on a new advisory on securing merchant payment terminals and remote access.

Last week, we released a joint advisory with the FBI and USSS on a type of wire transfer fraud called "business email compromise". "Business e-mail compromise" involves the compromise of legitimate business e-mail accounts for the purpose of conducting an unauthorized wire transfer. After a business e-mail account is compromised (often times a Chief Executive Officer or Chief Financial Officer), fraudsters use the compromised account or a spoofed account to send wire transfer instructions. The funds are primarily sent to Asia, but funds have also been sent to other countries all over the world.

The FS-ISAC participates in a variety of information sharing and other strategic programs, including the following:

- The FS-ISAC embedded a representative on DHS' National Cybersecurity and Communications Integration Center (NCCIC) watch floor two years ago. FS-ISAC representatives, cleared at the Top Secret / Sensitive Compartmented Information (TS/SCI) level, attend the daily briefs and other NCCIC meetings to share information on threats, vulnerabilities, incidents, and potential or known impacts to the financial services sector. Our presence on the NCCIC floor has enhanced situational awareness and information sharing between the financial services sector and the government, as well as other critical sectors.
- FS-ISAC representatives sit on the Cyber Unified Coordination Group (Cyber UCG), and the group has been actively engaged in incident response. The Cyber UCG's handling and communications with various sectors following the distributed denial of service (DDOS) attacks on the financial sector in late 2012 and early 2013 is one example of how this group is effective in facilitating relevant and actionable information sharing.
- The FS-ISAC, in conjunction with partner association and government agencies, has been involved in planning and executing a series of sector-wide cyber exercises that test our ability to share information and respond to critical incidents collaboratively with our government partners. In response to some of the conclusions from recent exercises, the FS-ISAC has launched a task force with over 80 representatives from the financial

services sector and numerous government agencies to develop best practices on how to mitigate and respond to a potential destructive malware attack.

- Finally, the FS-ISAC and Financial Services Sector Coordinating Council (FSSCC) have worked closely with government agencies to obtain security clearances for key financial services sector personnel. These clearances have been used to brief the sector on new information security threats and have provided valuable information for the sector to implement effective risk controls to combat these threats.

SECURITY AUTOMATION: SOLTRA EDGE

In recognition of the need to speed the flow of threat intelligence, the FS-ISAC established a joint venture with the Depository Trust and Clearing Corporation (DTCC) in 2014 to develop an automated cyber threat information sharing capability known as "Soltra Edge." Soltra Edge decreases the time to decision and mitigation from weeks and days to hours and minutes by leveraging two standards that the Department of Homeland Security funded and the MITRE Corporation developed: Structured Threat Information eXpression (STIX™) and Trusted Automated eXchange of Indicator Information (TAXII™). Soltra Edge takes threat intelligence from a variety of sources, normalizes it, and prioritizes this data at network speeds, turning it into instant actionable intelligence. Since its launch in December 2014, Soltra Edge has been downloaded by thousands of organizations both within financial services and other sectors. Created by users for users, Soltra Edge is designed to dramatically reduce the time it takes for security analysts to process threat information.

Soltra Edge is voluntarily funded by contributions from 16 financial services companies. In fact, the support for funding Soltra Edge came directly with several CEOs of our member

companies who recognized the strategic importance of developing this capability more rapidly and encouraged others in the financial sector to provide funding.

THREAT ENVIRONMENT

The current cyber threat environment continues to evolve and intensify. Each day, cyber risk grows as attacks increase in number, pace, and complexity. Our members constantly adapt to this changing threat environment. We are no longer in the days wherein the threat was confined to individual hacktivists and fraudsters. We are now in an era of attacks by not only organized crime syndicates, but also nation-states and entities affiliated with terrorist operations. Correspondingly, the attacks have grown beyond webpage vandalism and fraud into large-scale, prolonged campaigns that threaten the availability of services to citizens and threaten the privacy and accuracy of their information.

Our sector is increasingly concerned with these threats, particularly with the potential for attacks that could undermine the integrity of the financial system through data manipulation or destruction. This growing threat affects all institutions in our sector regardless of size or type of financial institution (e.g., banks, credit unions, insurers, payment processes and brokerage, investment firms). Increasingly, and as we have recently witnessed, other sectors face these same threats.

Malicious cyber actors with increasing sophistication and persistence continue to target the financial services sector. These actors vary considerably in terms of motivation and capability,

from nation states conducting corporate espionage, to advanced cyber criminals seeking to steal money, to hacktivists intent on making political statements. Many cybersecurity incidents, regardless of their original motive, have the potential to disrupt critical systems.

There are numerous tactics that malicious cyber actors use to target institutions. Among these the following are concerning:

- Targeted spear-phishing campaigns. These fraudulent emails, which appear to be legitimate, trick users into supplying sensitive information such as passwords that can result of the theft of online credentials and fraudulent transactions.
- Ransomware attacks in which malware is downloaded that restricts access to an infected computer (often via encryption) until a ransom is paid (often in Bitcoin).
- Distributed denial of service (DDoS) attacks which can impede access to services for extended periods of time.
- Business email compromise which involves the compromise of legitimate business e-mail accounts for the purpose of conducting an unauthorized wire transfer. After a business e-mail account is compromised (often times a CEO or CFO), fraudsters use the compromised account or a spoofed account to send wire transfer instructions.
- Supply chain threats.
- Blended physical and cyber attacks. An example of this is the theft of card data that is then used to steal money from ATMs around the globe using individuals who serve as "money mules".
- Insider threats.

The quote often attributed to Willie Sutton that he robbed banks "because that's where the money is" reminds us as to why financial institutions are often the subject of cyber-attacks. However, that quaint quote does not capture the entirety of the situation we face today. We also are observing that financial institutions are being targeted in response to international conflicts.

Perhaps the best visible example of this was the distributed denial of service attacks in 2012 through 2013 when an organization backed by a foreign country targeted dozens of financial institutions. The attacks were disruptive but they also resulted in unprecedented levels of information sharing among financial institutions and the US government. Information sharing proved to be extremely beneficial to firms that were targeted on the second, third and fourth wave of DDoS attacks given that the lessons learned from firms on the first wave were rapidly shared with others that had yet to be attacked. The DDoS attacks also led to increased collaboration with the major Internet Service Providers (ISPs) with financial institutions, facilitated by the FS-ISAC and BITS/Financial Services Roundtable.

The DDOS attack also catapulted the cybersecurity issue to a CEO level across the entire financial services sector for the first time. When the CEOs of our member financial services companies engaged directly it resulted in even greater collaboration among the financial associations and government agencies.

Being a focus of the attacks is certainly one reason why the financial sector has historically led the way in making huge investments in not only security infrastructure and the best-qualified

people to maintain the systems, but also in driving collaboration across industries and with the government. The primary reason for these investments is the recognition that customers trust financial institutions to protect them – to protect their investments, their records and their information. Individual financial institutions invest in personnel, infrastructure, services, and top-of-the-line security protocols to protect their customers and themselves and to respond to cyber-attacks. These investments protect the individual institutions and their customers, but on its own, an individual institution generally only has the ability to protect what is within its control. However, financial institutions are interconnected to others in the sector, with other sectors, and with the government. This reliance on others gives us in the financial services sector a unique and critical role in the cyber landscape and requires coordinated action for the most effective response. Recognizing the cyber threat environment continues to expand in complexity and frequency and that individual institution efforts alone will not be enough, executives from the financial services sector have stepped up efforts to work together.

RISK MANAGEMENT CULTURE, COLLABORATION AND REGULATION

In response to the changing threats, the FS-ISAC is working closely on risk mitigation strategies with numerous government agencies, including the U.S. Treasury Department, financial regulators, the Department of Homeland Security, and law enforcement agencies. These efforts build on the strong risk management culture within the financial services sector, in conjunction with extensive regulatory requirements.

Accordingly, we are striving to:

- Implement and maintain structured routines for sharing timely and actionable information related to cyber and physical threats and vulnerabilities among firms, across segments of the financial industry, and between the private sector and government and increasingly, to help properly share information between sectors.
- Improve risk management capabilities and the security posture of firms across the financial sector and the service providers they rely on by encouraging the development and use of common approaches and best practices.
- Collaborate with government agencies, other industry sectors, and international partners to respond to and recover from significant incidents.
- Discuss policy and regulatory initiatives that advance infrastructure resiliency and security priorities through robust coordination between government and industry.

We have learned that a strong risk management strategy for cyber and physical protection involves creating communities of trust in which professionals appropriately share information about threats, vulnerabilities, and incidents affecting those communities. That strategy is based on the simple concepts of strength in numbers, the neighborhood watch, and shared situational awareness. Sharing this information helps to prevent incidents from occurring and to reduce the risk of a successful incident at one firm later impacting another. These efforts increasingly focus on including smaller firms and international partners into the trusted community.

The financial sector is correctly credited with having a robust cyber security risk management culture. This is due, in part, to the fact that financial services are heavily regulated, and also to

the overarching imperative that our business models, consumer confidence, and the stability of the financial system and the global economy are dependent upon a secure and resilient infrastructure.

I certainly don't want to leave you with the impression that the financial sector needs more regulation to address the security challenge. Title V of the Gramm-Leach-Bliley Act of 1999 (GLBA) directed regulators to establish standards for financial institutions to protect customer information. Pursuant to GLBA, regulators have imposed broad information security requirements for regulated financial institutions with strong enforcement authority. In addition to issuing regulations over a decade ago, the federal financial regulators have issued extensive "supervisory guidance" that outlines the expectations and requirements for all aspects of information security and technology risk issues, including authentication, business continuity planning, payments, and vendor management." Regulators, for example, have imposed detailed requirements mandating strong internal procedures, vigorous threat and risk assessments, ongoing testing and evaluation of security systems, and required reporting to senior management and directors. Among the obligations to secure systems and protect data under GLBA and supervisory guidance, financial institutions must:

- Develop and maintain an effective information security program tailored to the complexity of its operations;
- Conduct thorough assessments of the security risks to customer information systems.
- Oversee service providers with access to customer information, including requiring service providers to protect the security and confidentiality of information;

- Train staff to prepare and implement information security programs;
- Test key controls, systems, and procedures and adjust key controls and security programs to reflect results of such ongoing risk assessments;
- Safeguard the proper disposal of customer information; and
- Update systems and procedures taking into account, for example, technology changes, emerging internal or external threats to information, changing business arrangements (e.g., mergers and acquisitions), personnel changes, and more.

It is also important to remind the Committee that financial institutions must comply with cybersecurity requirements and guidance from numerous regulatory bodies depending on their charter and activities. These regulatory bodies include the Commodity Futures Trading Commission, (CFTC), Consumer Financial Protection Bureau (CFPB), Federal Deposit Insurance Corporation (FDIC), Federal Reserve Board (Fed), Financial Industry Regulatory Authority (FINRA), Office of the Comptroller of the Currency (OCC), Securities and Exchange Commission (SEC), and numerous state banking agencies.

While regulatory requirements are a powerful and effective way to ensure that financial institutions have adequate controls in place, a growing challenge facing financial institutions today is the need for greater coordination and harmonization among the regulatory agencies, within the US and globally, to keep pace with new threats, new financial business process models, and the necessary skill sets to evaluate the intersection of those two for security and resiliency purposes. A common refrain we hear from senior executives and practitioners alike is

the need for regulators to harmonize regulatory requirements at both the policy and examination levels in order to reduce unnecessary regulatory compliance burdens and to better focus limited resources to mitigate cyber risks. While there are important efforts to coordinate among the independent regulatory agencies, more can and should be done to enhance regulatory coordination so that financial institutions are properly focused on enhancing security and resiliency and minimizing unnecessary regulatory burden.

It is also worth noting that financial institutions that handle payment information are also required to comply with non-regulatory standards, such as the Payment Card Industry Data Security Standard (PCI DSS). This also adds to the compliance burden to financial institutions as well as merchants and other organizations that handle payment information.

While not a regulatory requirement, regulatory agencies are reviewing the National Institute of Standards and Technology (NIST) Cybersecurity Framework to determine whether and how to harmonize and align regulatory requirements. The NIST Cybersecurity Framework was released in February 2014 in response to Executive Order 13636 of 2013 "Improving Critical Infrastructure Cybersecurity." The executive order directed NIST to seek private sector input through a collaborative process in developing a voluntary cybersecurity framework for critical infrastructure sector.

The Framework is a good example of public-private sector collaboration. NIST's successful approach at inclusion of so many essential parties reflects how broadly the Framework has been embraced by so many sectors. It synthesizes a process for cyber risk management that is

accessible from the boardroom to the operations floor, across not only individual enterprises but also entire sectors. It is a "Rosetta Stone" in that it provides a common lexicon for categorizing and managing cyber risks across sectors and enterprises for various unifying risk management jargons and creates a common understanding around various risk management terms, methodologies, ideas and language. It relies on international standards and is consistent with the regulatory requirements that have been in place for our sector for more than a decade. Down the road, the Framework has the potential to act as a baseline standard for cyber-insurance underwriters which could benefit multiple sectors by encouraging more secure and resilient cyber controls.

HOW CONGRESS CAN HELP

While the FS-ISAC and other information sharing organizations can provide many legal protections through member agreements, procedures and technologies, effective cyber threat information sharing legislation would enhance these capabilities to better match the increasing cyber threats that the public and private sectors face by providing targeted liability and disclosure protections. Effective cyber threat information sharing legislation includes the following elements:

- Facilitate real-time sharing to enable institutions and government to act quickly.
- Provide a targeted level of liability (such as a "good faith defense") and disclosure protections for cyber threat information sharing and receiving between individual institutions, through existing sharing mechanisms (such as the FS-ISAC), private to government, and government to private mechanisms.

- Provide protection from disclosure requirements through the Freedom of Information Act (FOIA), state sunshine laws, and to prudential regulators.
- Facilitate the appropriate declassification of information by the intelligence agencies and expedites the issuance of clearances to appropriate private sector individuals.

Bear in mind that the cyber threat information that the financial industry and lawmakers are talking about sharing are threat indicators that describe the type of malicious code sent to financial institutions, the route that malware took, and the means to protect it. This idea is very similar to law enforcement officials sharing data about physical crimes with the public and media outlets when a crime occurs or is attempted.

- What did the perpetrator look like?
- What kind of weapon was used?
- What did the getaway vehicle look like?
- Where did the criminals come from?
- Where did they go?

It is this type of information that, when shared, can be used to solve a crime or, perhaps more importantly, prevent more crime.

The Congress could also help by encouraging regulators to harmonize cyber security regulatory requirements.

In addition, the Congress could encourage the Administration to:

- Facilitate the appropriate declassification of information by the intelligence agencies;

- Expedite the issuance of clearances to appropriate private sector individuals;
- Recognize ISACs and the special operational role that they play in critical infrastructure protection and resilience and encourage owners and operators of critical infrastructure to join their respective sector ISACs;
- Support private sector efforts to form Information Sharing and Analysis Organizations (ISAOs) in the very few critical infrastructure sectors where they do not currently exist;
- Encourage all of the ISACs be represented on the NCCIC floor; and
- Recognize the National Council of ISACs as the coordinating body for the ISACs

CONCLUSION

Each week, more businesses, government agencies, and customers are victims of cyber attacks. The private sector is obviously waging a battle against adversaries whether they are launched by organized crime, organizations supported by other nations, or hacktivists. The FS-ISAC is responding by expanding our capabilities to share information in an automated way and to build stronger partnerships within the financial sector, with other sectors, with government agencies and with global partners. While the financial sector is an example of strong and frequent cyber collaboration and investment, we cannot fight this battle alone. Congress and the Administration can play a constructive role by enacting cyber threat information sharing legislation, encourage financial regulators to harmonize regulatory requirements, and support other efforts to enhance information sharing and cyber protections.

Appendix: Understanding FS-ISAC Communications

Understanding FS-ISAC Emails and Alerts

Determining which information is of value to your organization is one FS-ISAC cannot know. We can however, assist in providing you with guidance in parsing and forwarding FS-ISAC Alerts.

The email "subject" line in FS-ISAC alerts sent to the membership uses the following format

- ***[Alert_Type][Criticality]: [Alert_Title]***

Depending on your role, you don't have to follow every update, but FS-ISAC recommends following these key reports. Doing so will limit emails to about 10/day

Step 2: *Understand the Criticality and Priority*

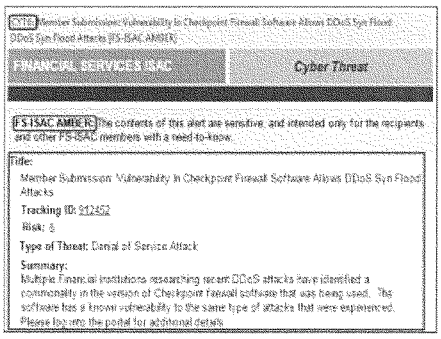
- ANC = Priority – 1-10, 8-10 is high priority
- CYV = Risk – 1-10, 8-9 is Urgent, 10 is Crisis
- CYT = Risk – 1-10, 8-9 is Urgent, 10 is Crisis
- COI – No Criticality Metric
- PHT = Risk – 1-10, 8-9 is Urgent, 10 is Crisis

Step 3: *Make Choices Based on role*

- Analysts and those involved in risk assessment or vulnerability/patch management should receive CYV alerts.
- Intelligence analysts may also want to participate on the Cyber Intel listserv. POCs are automatically added, but a portal account is not necessary if you wish to add additional analysts to the distribution.
- Provide portal accounts to your staff based on each individual's role. This will allow them to employ portal filtering for their unique assignments.
- We provide summary reports for mangers and technical reports for analysts. Making informed choices based on your role eliminates unneeded emails.

FINANCIAL SERVICES ISAC

Key Components of Alerts



The abbreviation and criticality level will always appear in the subject line, along with the title

Be aware of FS-ISAC's Traffic Light Protocol

Following the TLP Color, the alert will go into more detail such as the type of threat, summary, and handling instructions

FINANCIAL SERVICES ISAC

Congressional Testimony

Evaluating the Security of the U.S. Financial Sector

Chip Poncy
Senior Advisor, Center on Sanctions and Illicit Finance
(CSIF), Foundation for Defense of Democracies
Founding Partner, Financial Integrity Network

House Financial Services Committee
Task Force to Investigate Terrorism Financing

Washington, DC
June 24, 2015

Center on Sanctions
& Illicit Finance
FOUNDATION FOR DEFENSE OF DEMOCRACIES
1726 M Street NW • Suite 700 • Washington, DC 20036

Chip Poncy 6/24/2015

Chairman Fitzpatrick, Vice Chairman Pittenger, Ranking Member Lynch, and other distinguished members of the Task Force, I am both humbled and honored by your invitation to testify today at this third hearing of the Task Force to Investigate Terrorism Financing. Your work is tremendously important, not only to our national and global security, but also to our financial integrity and economic prosperity.

Introduction

I was extraordinarily privileged to serve our country at the United States Department of the Treasury for 11 years following the terrorist attacks of 9/11. I worked with and for an immensely talented and dedicated group of individuals from across the government. This was a pivotal period in the development and institutionalization of an unprecedented global campaign to counter the financing of terrorism (CFT).

From the time of 9/11 through the present, the United States has led this global CFT campaign with unprecedented tenacity and commitment. This commitment has been vindicated by the substantial disruptive and preventive impact of our CFT efforts against our most pressing terrorist threats. Due to these successes, the ongoing global CFT campaign is now unquestionably recognized as a pillar of the broader counter-terrorism mission. Nearly 14 years after the inception of the modern CFT campaign, the ongoing work of this Committee and Task Force is a testament to this fact.

And yet the CFT challenges facing us now are perhaps greater than ever before. The rise of the Islamic State and the resiliency of a balkanized, but continually dangerous, al Qaeda and its global network of affiliates demonstrate the ongoing urgency of the terrorist threat. As we have succeeded in clamping down on more overt forms of support to terrorist organizations, these and other terrorist groups have adjusted their means of obtaining the resources they need.

Many of these terrorist financing methods are not new, but they have become more pervasive. Prominent examples include the rise of kidnapping for ransom and the other criminal activities, increasingly in collaboration with criminal organizations. Fundraising and recruitment over the internet and exploitation of local economies under terrorist control have also grown, exposing limitations of our CFT approach. And despite the potential of a nuclear deal, Iran's continued and aggressive state sponsorship of terrorism presents complex but urgent challenges to the global CFT campaign.

To meet these challenges, we must adjust our CFT campaign to directly confront the shifting terrorist financing methodologies of today's primary terrorist threats. This will no doubt include continued development and adaptation of our CFT operational and targeting capabilities. More fundamentally, this must also include addressing systemic challenges to our financial security. Such challenges increasingly undercut the effectiveness and threaten the sustainability of the global CFT campaign.

My remarks today will focus on these systemic challenges. Such challenges are not new, nor are they limited to the CFT campaign or to the United States. But addressing these systemic challenges is more important than ever before, not only for our CFT campaign, but also for our national and collective security, and for our economic stability.

Addressing these challenges will require us to strengthen global commitments to financial integrity, including through continued implementation and enforcement of global anti-money laundering (AML)/CFT standards and financial sanctions regimes. These are global standards that sustained US leadership has helped to create. The integrity of our financial system relies on their effective implementation, as well as our continued development and application of targeted financial measures.

This ongoing work to strengthen and protect U.S. and global financial integrity will clearly require the continued leadership of the United States and the strong support of this Committee.

I will begin with a brief explanation of the meaning of financial integrity and its importance in today's evolving CFT campaign and to our broader security and economic interests. I will also highlight how the global AML/CFT and financial sanctions regimes led by the United States over the past generation have helped create a foundation of financial integrity essential to the work that lies ahead. I will then outline the key systemic challenges to financial integrity, including with respect to financial transparency and financial accountability. I will close with a series of recommendations for actions that this Committee can take to address these challenges.

The Financial Integrity Imperative

Financial integrity is fundamentally about financial transparency and accountability. These concepts provide the foundation upon which our CFT campaign and broader counter-illicit financing mission rest. They are also crucial to protecting our financial system, national security, and economic interests. And they rely upon effective implementation of global AML/CFT and financial sanctions standards.

Financial Transparency

Financial transparency is crucial to financial integrity because it allows us to identify, track and trace the sources, conduits and uses of terrorist financing that transit the financial system. This is equally true for all manner of illicit finance. Without financial transparency, financial institutions and regulators cannot identify, manage or avoid risks ranging from financing al Qaeda to brokering nuclear proliferation to banking corruption. Law enforcement cannot track or trace progressively globalized criminal networks or their illicit proceeds. States cannot identify or recover stolen assets or proceeds of tax evasion. And financial pressure to address gross violations of international law by Iran, Syria, Russia or others becomes a hollow talking point rather than an operational instrument of global security.

Certainly, financial transparency alone cannot satisfy these needs. But without it, these needs cannot be met. This is why financial transparency is both a core objective of the global counter-illicit financing community and a driving principle of financial reform by the G20 and the G7.

Accountability

Accountability is crucial to financial integrity because it gives us confidence that the rule of law is enforced across the financial system. With respect to combating illicit finance, accountability drives financial integrity in two respects. First, accountability is needed to enforce requirements of and responsibilities for financial transparency across the financial system, including with respect to the customers, institutions and ultimately the authorities that access, service and govern the financial system. Second, accountability is needed to pursue, disrupt, punish and deter those who abuse the financial system in pursuit of illicit activity. It is essential to recognize that failure of accountability in either of these two respects undermines the integrity of the financial system.

Economic Stability

Beyond the clear national security imperatives of financial transparency and accountability, financial integrity is also essential to protect our economic stability. When financial transparency and accountability suffer, the integrity of economic markets can erode, and with it market confidence. Short term gains associated with short-cuts around systemic investments in financial integrity are ultimately a losing proposition. When investors realize that their capital is not protected by the integrity of financial markets, they lose confidence in their investments. And they move their capital to markets whose integrity protects their interests. This is particularly true when times are turbulent.

The U.S. market has thrived historically in part because of the integrity of our financial system. The financial transparency and accountability created by the sound implementation of AML/CFT and financial sanctions regimes play an increasingly important role in protecting the integrity of not only our financial system, but also of the economy it supports. The financial transparency and accountability fostered by AML/CFT and financial sanctions regimes guard our economy from various forms of corruption that undermine market principles. Such regimes, when properly implemented and enforced, help protect the market integrity of industries that enjoy the public trust and the confidence of investors. When such regimes are absent, market integrity is threatened.

The globalization of market economies underscores the importance of enforcement actions against those who fail to implement AML/CFT and financial sanctions regimes. Countries and financial institutions with systemic deficiencies in their AML/CFT and financial sanctions regimes present systemic vulnerabilities to the integrity of the international financial system and the global economy it supports. In an increasingly globalized financial system and economy, such deficiencies in any one country or

financial institution present vulnerabilities to other countries and institutions. They also present vulnerabilities to the industries, investors, depositors and other customers they service. Ultimately, these vulnerabilities can jeopardize the health of the general economy.

In an increasingly globalized financial system, economy and threat environment, our financial integrity requires a global commitment to financial transparency and accountability. For decades, the United States has led the development of a comprehensive and global counter-illicit financing framework. This framework is designed to achieve the financial transparency and accountability upon which our CFT campaign and collective security increasingly depend. As discussed below, this global framework represents an accomplishment as tremendous as it is important, providing a financial integrity foundation that is both deep and wide. The financial integrity imperative must now focus on strengthening implementation of the key measures that deliver financial transparency and accountability pursuant to this global framework.

This first requires a brief explanation of the global counter-illicit financing framework as a foundation for securing our financial integrity.

A Global Foundation for Financial Integrity

After 9/11, the global CFT campaign led by the United States became an instrumental factor in accelerating a global understanding of the importance of financial integrity to our collective security. Protecting the integrity of the financial system has since become central to the mission of the United States Department of the Treasury and to that of finance ministries around the world. Through the work of the G7, the G20, the Financial Action Task Force (FATF), eight FATF-Style Regional Bodies (FSRBs), the World Bank, the IMF and the United Nations, the United States has led a global commitment to protecting the integrity of the financial system against all manner of illicit finance.

This commitment is evident in the rapid evolution of the global counter-illicit financing framework. This framework continues to drive development and implementation of comprehensive jurisdictional AML/CFT, counter-proliferation and financial sanctions regimes. This framework, largely led by the work of the FATF, manages jurisdictional participation in conducting the following sets of activities:

- Developing typologies of illicit financing trends and methods;
- Deliberating counter-illicit financing policies and issuing global counter-illicit financing standards;
- Conducting and publishing regular peer review assessments of jurisdictional compliance with the FATF's global standards; and
- Managing follow-up processes that both assist jurisdictions and hold them accountable in implementing the FATF standards.

Through the FATF network of assessor bodies, the overwhelming majority of countries around the world are incorporated into this counter-illicit financing framework.

The global standards issued by the FATF and assessed through this global framework cover a broad range of specific measures to protect the integrity of the financial system from the full spectrum of illicit finance – including money laundering, terrorist financing, proliferation finance, serious tax crimes, and corruption. These global standards create a conceptual and technical roadmap for countries and financial institutions to develop the capabilities required to advance and secure the integrity of the global financial system. The FATF standards generally encompass the following areas:

- Jurisdictional and financial institution processes and policies to assess and address illicit financing risks;
- Preventive measures covering the entirety of the financial system;
- Transparency and beneficial ownership of legal entities, trusts and similar arrangements;
- Regulation and supervision;
- Targeted financial sanctions;
- Criminalization of money laundering and terrorist financing;
- Confiscation of criminal proceeds;
- Financial analysis and investigation; and
- International cooperation.

Implementing the FATF global standards within and across these different areas of importance requires a whole-of government approach in collaboration with the private sector, particularly financial institutions. It is a massive undertaking. And it is essential to protect the integrity of the financial system.

Peer review assessments over the past several years demonstrate that most countries have taken substantial steps towards implementing many if not most of the requirements covered by the FATF global standards. Collectively, this work represents a tremendous accomplishment in creating a firm global foundation for financial integrity.

Nonetheless, these comprehensive jurisdictional assessments also reveal a number of deep-seated, systemic challenges to financial integrity. These challenges are also evident from many of the U.S. enforcement actions taken against global financial institutions in recent years, as well as from consistent criminal typologies of illicit finance. Such challenges may be broadly divided between those that undermine financial transparency and those that threaten financial accountability.

Systemic Challenges to Financial Transparency

Financial transparency generally requires implementation of the full range of preventive measures included within the FATF global standards. Ongoing systemic challenges to financial transparency primarily stem from important gaps in implementing these preventive measures, including in particular:

(i) Effective customer due diligence by financial institutions;

(ii) Meaningful beneficial ownership disclosure and maintenance requirements for legal entities;

(iii) AML/CFT coverage of the complete financial system; and

(iv) Information-sharing to enable financial institutions to understand and manage correspondent or intermediated illicit financing risks.

These measures, and the systemic challenges that frustrate their implementation, are briefly discussed below.

Customer Due Diligence

Financial transparency fundamentally requires financial institutions to understand the persons and entities with whom they do business, whether on an ongoing or occasional basis. Customer due diligence (CDD), or know-your-customer (KYC) rules, are commonly understood as the bedrock of financial transparency.

Pursuant to FATF global standards, CDD/KYC generally includes the following four elements: (i) customer identification and verification; (ii) beneficial ownership identification and verification; (iii) understanding the nature and purpose of the customer account or relationship, and (iv) monitoring customer account activity. Failure to implement any of these required elements undermines financial transparency, making it more difficult to identify, track or trace illicit financing networks.

Each of these four elements of CDD can present challenges for financial institutions, but the consistent lack of beneficial ownership information collected by financial institutions has historically posed a systemic vulnerability undermining financial transparency. To be effective, CDD obligations must go beyond identifying the front companies, shell companies and other cut-outs frequently used to open accounts on behalf of criminals. Addressing this common method of illicit finance requires gathering meaningful information about the beneficial owners of financial accounts – that is, the primary individuals who ultimately own, control or benefit from these accounts.

In accordance with FATF global standards, financial institutions should be required to obtain such information from their customers as a routine element of CDD. Customers that fail to provide such information should be denied access to the financial system. Customers that deliberately misrepresent such information for purposes of avoiding detection should be subjected to meaningful sanctions, including prosecution for fraud.

In recent years, most financial centers have significantly strengthened CDD requirements for financial institutions, including for purposes of specifically addressing shortcomings in beneficial ownership information collection. However, implementation and enforcement of these requirements, particularly in non-bank financial institutions, remains a systemic challenge. In some countries, including the United States, beneficial ownership information is not yet required as a routine element of CDD. The systemic

vulnerabilities created by these weaknesses in CDD substantially compromise financial transparency.

Beneficial Ownership Requirements for Legal Entities

In higher risk scenarios, financial institutions should verify the beneficial ownership information obtained from their customers through independent corroboration of the beneficial owner's status. This presents significant challenges for financial institutions that lack independent sources of information about their legal entity customers. To assist financial institutions in conducting such verification, countries should demand beneficial ownership information as a condition for granting legal status to those entities formed under their authorities.

Equally importantly, beneficial ownership requirements for legal entities will provide immensely valuable information for law enforcement and other authorities. An abundance of testimony and evidence over the past several years demonstrates that investigations of legal entities implicated in all manner of criminal activity are all too often frustrated by of a lack of meaningful beneficial ownership information.

For these reasons, the FATF global standards clearly require jurisdictions to impose beneficial ownership disclosure and maintenance requirements for legal entities formed under their authorities. Yet few jurisdictions require companies to disclose their beneficial ownership as a condition of obtaining or maintaining their legal status. Of those jurisdictions that do require such disclosure, few have meaningful verification or enforcement processes to ensure the credibility of the beneficial ownership information they collect. This consistent lack of available and credible beneficial ownership information for legal entities – in the United States and most financial centers around the world – presents another systemic challenge undermining financial transparency.

AML/CFT Coverage of the Complete Financial System

Financial transparency is complete only to the extent that it applies across the entire financial system. All financial institutions – including non-banking financial institutions such as broker dealers, investment advisors, and money services businesses – should be subjected to effective AML/CFT regulation. In addition to non-bank financial institutions, certain industries that can operate as de-facto financial institutions or that facilitate access to financial services for their customers may present systemic vulnerabilities to illicit finance. Such industries include casinos, real estate agencies, dealers in precious metals and stones, and trust and company service providers.

Failure to extend meaningful AML/CFT regulation to these non-bank financial institutions or vulnerable industries can allow illicit financing networks to obtain the financial services they need without detection. Once illicit actors gain access to any part of the financial system, the highly intermediated nature of the system facilitates their access to other parts, including by sector or geography.

Any unregulated or under-regulated financial sector or vulnerable industry also puts more pressure on those sectors that are regulated. It is much more difficult to detect illicit financing risks that are intermediated through another financial institution or through a customer or account that represents unknown third party interests. Correspondent relationships with unregulated financial institutions or vulnerable industries that lack AML/CFT controls allow criminals to access even well-regulated financial institutions through the back door.

For this reason, correspondent relationships are generally considered high risk under FATF global standards, even between financial institutions that are well-regulated for AML/CFT. Correspondent relationships with financial institutions that lack AML/CFT regulation may be prohibitively high risk. The same may also be true of accounts with businesses from other vulnerable industries that lack AML/CFT regulation.

In light of these concerns, FATF global standards direct countries to extend AML/CFT preventive measures across all financial sectors and vulnerable industries, including the legal and accounting professions. Covering all of these sectors and industries can challenge considerable political interests and entails substantial costs. As a result, many countries, including the United States, lack full AML/CFT coverage of their financial systems or vulnerable industries. These gaps in coverage put more pressure on banks and other sectors that are covered and present systemic challenges to financial transparency.

Intermediation and Information-Sharing

Illicit financing networks, like the business of most enterprises, almost always implicate more than one financial institution. Whether in the process of raising, moving, using or laundering funds associated with illicit activity, such networks almost invariably transact across multiple financial institutions. For the illicit financing networks of most pressing concern, transactions also often cross multiple jurisdictions. Identifying, tracking and tracing these networks therefore depends critically upon information-sharing across financial institutions and across borders.

FATF global standards require or encourage countries and financial institutions to share information in many ways. However, implementation of such information-sharing measures is routinely constrained or prohibited by data protection, privacy, or business interests, or by liability concerns associated with these interests. Many counter-illicit financing professionals in governments and in financial institutions consider data protection and privacy to be the "new bank secrecy" that was the genesis for much of interest in creating the FATF over 25 years ago.

The systemic challenge posed by these information-sharing constraints is perhaps most evident in the risk management programs of global banks and large financial groups. FATF global standards direct countries to require such banks and financial groups to develop risk management programs that cover their entire enterprise. The wide scope of these programs is deliberately aimed at identifying and addressing illicit financing risks across all branches and affiliates of the bank or financial group, wherever located. Yet

data protection, privacy and other restrictions in many countries prohibit such banks or financial groups from sharing much of the information that is relevant or even essential to such enterprise-wide risk management programs. These restrictions apply even when the information sought is intended to be kept entirely within the financial group's enterprise.

Even more problematic for these institutions, information-sharing requirements and prohibitions from different countries can conflict with one another, making it impossible to comply with the laws or expectations of different financial centers in which global banks and financial groups operate.

Information-sharing challenges associated with financial intermediation and illicit finance are not limited to cross-border scenarios or to risk management programs. Even within jurisdictions, many of the same constraints prevent financial institutions from sharing information that can be critical in identifying or addressing illicit financing risks. This presents opportunities for countries, including the United States, to begin understanding and addressing these challenges through domestic information-sharing enhancement processes, in partnership with their financial institutions.

The sensitivity of financial information and the legitimate interests behind data protection and privacy raise important considerations for policymakers in determining how best to address these information-sharing challenges. Although more work is needed to better understand these challenges and how best to overcome them, it is clear that the lack of proactive or even reactive information-sharing between and among financial institutions presents a systemic challenge to financial transparency.

Systemic Challenges to Financial Accountability

Distinct and global systemic challenges to financial accountability exist with respect to both achieving compliance with financial transparency requirements and pursuing and disrupting illicit financing networks. I will focus primarily on those systemic challenges that directly implicate financial authorities.

Achieving Compliance with Financial Transparency Requirements

Over the past several years, the United States and most countries have undertaken substantial efforts to strengthen and expand AML/CFT preventive measures required to achieve transparency across the financial system and other vulnerable industries. Yet in all jurisdictions, implementation of these measures remains a constant challenge. This is overwhelmingly due to the complexity of the financial system, the global economy, and of illicit financing networks and schemes.

In many instances, however, such challenges of global implementation may also be owing to the lack of effective enforcement and an ensuing lack of compliance culture in the private sector regarding AML/CFT preventive measures. In turn, these industry compliance concerns implicate questions of industry supervision. These issues present

distinct and global systemic challenges of financial accountability associated with achieving compliance with financial transparency requirements.

1. Challenges of Industry Compliance

As a general matter, U.S. enforcement of AML/CFT preventive measures is particularly strong. A long string of U.S. enforcement actions against global banks and other financial institutions in recent years underscores the U.S. commitment to the global AML/CFT regime and financial integrity. At the same time, these enforcement actions have raised questions about the state of industry compliance with AML/CFT preventive measures, both within the United States and particularly abroad.

Many of these enforcement actions reveal systemic deficiencies in AML/CFT policies, procedures, systems and controls, including in many of the world's largest and most well-regulated banks. The immense size and complexity of these banks, and the corresponding illicit financing risks they must manage, help explain the particular focus of AML/CFT authorities in making sure these banks implement effective AML/CFT measures, including those that provide financial transparency. It also helps explain the need for more sophisticated AML/CFT programs that implicate particular compliance challenges in these banks.

However, the fundamental breakdowns that have given rise to these enforcement actions raise important concerns about the general culture of compliance with AML/CFT preventive measures across the core banking sector. This continues to be a dominant topic of concern to U.S. authorities, and is beginning to resonate in other financial centers.

This realization has prompted efforts in the United States, and in some instances in other financial centers, to intensify AML/CFT oversight of key financial institutions. U.S. authorities have placed many of the world's largest financial institutions operating in the United States under intense monitoring and oversight programs as a key condition for settling various AML/CFT enforcement actions. It is unclear whether similar efforts may be underway to the extent that may be required in other financial centers. This is particularly true with respect to non-banking sectors.

Given the importance of this issue and its relatively recent focus, it is also unclear what systemic changes in the AML/CFT culture of compliance across key financial sectors and centers may ultimately result from these efforts. However, it is apparent that the enforcement actions taken by the United States to strengthen compliance with AML/CFT preventive measures and financial sanctions have made a substantial impact, particularly in the global banking sector. The combination of enforcement and outreach by U.S. authorities, particularly in recent years, has led many financial institutions to adopt important structural, policy and programmatic changes that have substantially improved their ability to understand and manage illicit financing risks. This work must continue.

Notwithstanding the significant progress achieved by financial institutions in strengthening compliance with AML/CFT preventive measures and financial sanctions, questions of compliance continue to present an ongoing global and systemic challenge of financial accountability. This may be particularly true in other financial centers that lack the strong enforcement actions taken by the United States.

2. Challenges of Industry Supervision

The above concerns of global industry compliance with AML/CFT preventive measures have also raised global challenges of AML/CFT financial supervision. These supervisory challenges broadly include: (i) the appropriate role of law enforcement in facilitating industry compliance; (ii) supervisory coordination, particularly for larger financial groups that often have multiple regulators in multiple jurisdictions, and (iii) the effectiveness of existing supervisory AML/CFT models in money services businesses (MSBs) and other non-banking or non-financial sectors lacking a functional financial regulator.

In the United States, as in most financial centers, financial functional regulators bear the primary responsibility for examining and ensuring compliance with AML/CFT preventive measures across the covered financial sectors they supervise. In administering this responsibility, U.S. federal and state regulators continue to pursue more active cases of AML/CFT enforcement than any of their financial counterparts around the world, strengthening AML/CFT compliance across the international financial system.

The strong AML/CFT enforcement record of financial functional regulators in the United States has been critically supported by the prominent and unique role of U.S. federal and state law enforcement in enforcing global compliance with AML/CFT preventive measures. These law enforcement authorities are a driving factor in strengthening the integrity of the global financial system.

The essential role of U.S. law enforcement in enforcing global compliance with AML/CFT preventive measures raises systemic challenges of financial accountability on a global level. Other countries, including those whose financial institutions have branches subjected to AML/CFT enforcement actions in the United States, should consider whether compliance with AML/CFT preventive measures in their jurisdictions could be strengthened by giving their AML/CFT law enforcement agencies a more active role in enforcing compliance.

Inside the United States, the compliance enforcement role of law enforcement raises systemic challenges of how best to coordinate law enforcement's independent investigative authority with the independent supervisory authority of U.S. regulators. Such coordination is essential to provide financial institutions with a clear, consistent and reasonable set of AML/CFT expectations that they must meet to effectively implement their AML/CFT obligations. This is particularly true when considering the necessary discretion that financial institutions must have to manage illicit financing risks. Such

discretion is essential to preserving the risk-based approach that guides U.S. and global implementation of AML/CFT preventive measures.

In 2012, the United States Department of the Treasury began to address these concerns and related issues through the work of a federal AML Task Force that included the Department of Justice and the financial functional regulators. This Task Force developed a number of initiatives to strengthen coordination among federal law enforcement and financial regulatory authorities on a wide range of AML/CFT matters. These initiatives were generally designed to facilitate a common understanding of the illicit financing risks facing the U.S. financial system and align corresponding risk management expectations in supervising and enforcing compliance with AML/CFT preventive measures.

Such initiatives likely assisted the Department of the Treasury in developing the 2015 National Money Laundering and Terrorist Financing Risk Assessments issued earlier this month. These risk assessments provide incredibly valuable information to financial institutions and all AML/CFT stakeholders about the money laundering and terrorist financing threats, vulnerabilities and risks currently facing the United States and our financial system.

The initiatives of the AML Task Force will become important in aligning law enforcement and supervisory expectations for financial institutions that must consider the National Money Laundering and Terrorist Financing Risk Assessments in developing their own illicit financing risk assessment and risk management programs.

The systemic challenge of aligning supervisory expectations is exacerbated for larger financial groups that often have multiple regulators in multiple jurisdictions. In managing differences in AML/CFT requirements between home and host countries of financial groups, FATF global standards direct such groups to apply the laws of the jurisdiction with the stronger requirements. To support this outcome, or any outcome with consistency, supervisors across jurisdictions and across sectors must have a system for coordinating their efforts. The initiatives of the AML Task Force may help illuminate ways of standardizing and strengthening these efforts.

Supervisory AML/CFT models for sectors that lack a functional financial regulator present yet another systemic supervisory challenge to financial accountability. In the United States, as in most other financial centers, MSBs and certain other non-banking or non-financial sectors covered under existing AML/CFT preventive measures lack a federal functional regulator. This raises substantial challenges of resources and expertise needed to oversee effective implementation of AML/CFT preventive measures in these sectors.

To address these challenges, the United States and many other countries delegate national AML/CFT examination authority for these sectors to national or federal tax authorities. While there continue to be reasonable arguments defending this position, it is becoming increasingly clear that additional examination and/or supervisory support may be needed to adequately oversee effective AML/CFT implementation in these sectors.

The United States continues to develop and explore initiatives to strengthen oversight and examination of these sectors through the Financial Crimes Enforcement Network (FinCEN). FinCEN is a Treasury bureau that functions as the U.S. financial intelligence unit and additionally has authority delegated from Treasury to issue and enforce AML/CFT preventive measures across the U.S. financial system in accordance with the Bank Secrecy Act (BSA).

In particular, FinCEN has coordinated with and leveraged MSB licensing and examination authorities in most states. FinCEN also continues to coordinate with Treasury's Internal Revenue Service in pursuing a principal-agency model for MSB examination. This model consolidates AML/CFT responsibility for MSB agent networks with their principals, including Western Union, MoneyGram, Sigue and other primary money transmitters.

It is unclear the extent to which other countries are developing or exploring these or other models for strengthening regulatory examination and oversight of AML/CFT preventive measures in sectors that lack a functional regulator. It is also not clear whether further steps may be needed to bring additional AML/CFT supervisory resources and expertise to these sectors.

What is clear is that MSBs and other sectors covered by AML/CFT regulation but lacking a federal functional regular – including insurance companies, casinos, and dealers in precious metals and stones in the United States – may present substantial risks of illicit finance. While the relative scale of these risks may appear small when compared to the overwhelmingly disproportionate size of the banking sector and capital markets, the high risk nature of the services offered by some of these sectors can make them disproportionately prone to illicit financing risks.

The recent emergence of virtual currency providers underscores this point. Virtual currencies and the administrators and exchangers that provide them have emerged as a potentially promising new form of money transmission. Yet this relatively new industry understandably lacks familiarity or experience with AML/CFT risk management. When these illicit financing risks are compounded by limited oversight and supervision, they can appear prohibitive to the banks that virtual currency providers, other MSBs and other AML/CFT covered industries ultimately rely upon for convertibility, settlement, clearance and other services. This can frustrate efforts to obtain banking services and in some instances may provide an additional impetus for banks to exit accounts with such industries.

Pursuing and Disrupting Illicit Financing Networks

Beyond ensuring compliance with AML/CFT preventive measures necessary to achieve financial transparency, financial accountability requires countries to effectively pursue and disrupt illicit financing networks. It is these networks, and the criminal interests they support, that ultimately undermine the integrity of the financial system.

There are a number of systemic challenges that the United States and all countries face in pursuing and disrupting illicit financing networks. As in the case of achieving financial transparency, these challenges primarily stem from gaps in implementing FATF global standards. Such standards broadly include requirements to facilitate effective analysis and investigation, prosecution and confiscation, and targeted financial sanctions against illicit financing activities, actors and assets. They also include a number of measures to facilitate cross-border cooperation in these actions.

The systemic challenges to pursuing and disrupting illicit financing networks presented by gaps in implementing FATF global standards are numerous and require additional time and consideration beyond the immediate scope of this hearing. However, it is important to recognize that the work of the FATF is now focused on assessing the effectiveness of jurisdictions in implementing AML/CFT and financial sanctions requirements pursuant to revised and strengthened global standards. This work, facilitated by the leadership of the United States and other financial centers, will greatly assist countries in identifying and closing gaps in implementing the FATF global standards, including those required to pursue and disrupt illicit financing networks.

Today, I would like to briefly highlight two critical developments that appear to have emerged from systemic challenges in pursuing and disrupting illicit financing networks.

The first development concerns the growing difficulty of systematically pursuing complex, cross-border criminal investigations of sophisticated illicit financing networks. The expertise and investment of time and resources required to systematically pursue such financial investigations is often prohibitive for all but the most advanced, well-resourced and protected teams of criminal investigators and financial analysts. The United States is consistently more effective in overcoming these challenges than any other country in the world. Nonetheless, these challenges are becoming more daunting as the complexity and globalization of the financial system and illicit financing networks have grown.

To keep pace with these challenges, the United States has increasingly turned to national security authorities to combat illicit financing and the transnational criminal organizations that often perpetrate and benefit from such activity. This is the second development that has emerged from the systemic challenges to pursuing and disrupting illicit financing networks. Just as terrorism and other national security threats have converged with criminal interests, so has our response.

To address the growing challenges that law enforcement faces in pursuing and disrupting illicit financing networks, the United States has developed effective complementary outcomes to criminal prosecution and forfeiture. These outcomes increasingly offer options for law enforcement, in collaboration with financial authorities, to effectively disrupt and deter sophisticated transnational organized crime through the application of targeted financial measures. These measures include targeted financial sanctions most often issued by Treasury under the International Economic Emergency Powers Act

(IEEPA) and preventive measures issued by Treasury pursuant to Section 311 of the USA PATRIOT Act.

The success of these authorities in assisting law enforcement pursue and disrupt an expanding range of transnational criminal activity illicit financing can be seen in the expansion of financial sanctions over the past several years. Such sanctions, originally applied against Columbian drug cartels and eventually global drug trafficking organizations, have expanded to target criminal conduct ranging from terrorist financing, proliferation financing, foreign corruption in context of certain sanctioned government regimes, and most recently, cybercrime.

The increasing application of targeted financial measures to disrupt an expanding range of criminal activity can also be seen in increased use of Section 311 to target primary money laundering concerns. These concerns include those presented by rogue digital currency providers, as well as money transmitters and banks that become infiltrated or exploited by organized crime and terrorist organizations.

Far from precluding more traditional outcomes of criminal prosecution and forfeiture, these actions can often facilitate such outcomes, as several cases have shown.

These developments underscore the importance of targeted financial measures to strengthen our financial integrity in combating the criminal and national security threats we face. They also underscore the acute need for ongoing U.S. leadership in continuing to advance the global commitment to financial integrity, including through the application of targeted financial sanctions and measures.

Recommendations to Address Systemic Challenges to Financial Integrity

Addressing the systemic challenges to financial integrity discussed above will require the clear support of this Committee. The following recommendations outline specific steps that this Committee can take to lead Congressional action, including with respect to new legislation, support for further executive action by the Administration, and targeted investments specifically directed to protect and strengthen our financial integrity against the full range of threats to our national and collective security.

New Legislation

Since the issuance of the USA PATRIOT Act in October 2001, the Congress has generally provided unwavering and essential bipartisan support and leadership on a wide range of issues to protect the integrity of the U.S. and international financial system. This is particularly true with respect to Congressional legislation. The following additional legislative action will further these interests by addressing systemic challenges to our financial integrity:

(i) Adopt legislation expanding the purposes of the Bank Secrecy Act (BSA) to explicitly include protecting the integrity of the financial system. Such

legislation is required to underscore the importance of financial integrity and the full partnership that is required between industry and authorities to achieve it. Section 5311 of Title 31 of the United States Code declares the purpose of the BSA "to require certain reports or records where they have a high degree of usefulness in criminal, tax, or regulatory investigations or proceedings, or in the conduct of intelligence or counterintelligence activities, including analysis, to protect against international terrorism." While this purpose is more important than ever, it is also incomplete. Protecting the integrity of the financial system is an essential objective in its own right.

Expanding the purpose of the BSA to reflect this will elevate the role of financial institutions and underscore the importance of government partnership with them. In addition to law enforcement and other investigative and analytic authorities, financial institutions – together with the customers and economy they service – are direct beneficiaries of financial integrity. They are also end users of BSA recordkeeping and reporting, relying on such information to identify and manage all manner of illicit financing risk for purposes of protecting the integrity of the financial system. And they must be full partners with governing authorities in implementing the BSA to advance this purpose.

Amending the purpose of the BSA will assist all stakeholders in recognizing these truths. It may also facilitate a stronger commitment to a risk-based approach by industry and authorities. Protecting the integrity of the financial system, beyond filing reports or maintaining records, clearly requires such an approach. This will further augment the importance of collaboration between industry and governing authorities to facilitate a shared understanding of illicit financing risk and effective risk management programs.

(ii) Adopt legislation to require the disclosure and maintenance of meaningful beneficial ownership information in company formation processes. Such legislation is required to address the systemic challenges posed by the chronic abuse of legal entities to mask the identities and illicit financing activities of the full scope of criminal and illicit actors. For several years and through at least three consecutive administrations, various arms of the Executive Branch – including several law enforcement agencies and the Department of the Treasury – have called for meaningful action on this issue. For an even longer period, the Senate Permanent Subcommittee on Investigations, beginning with the prior leadership of Senator Levin, has called for such action.

The current Administration has developed a proposal that is reasonable and effective, leveraging current IRS reporting requirements to obtain beneficial ownership information from companies created under the authority of the states. This Committee should work with the Congress, the Administration and state

authorities to support this approach, including through legislation required to ensure adequate availability of beneficial ownership information to the full range of US authorities investigating illicit finance.

(iii) Consider legislation strengthening the information-sharing provisions of Section 314 of the USA PATRIOT Act. Such action may assist in addressing the systemic challenges to financial integrity posed by information-sharing constraints. Such legislation could strengthen information-sharing by clearly extending Section 314(b)'s safe harbor provisions to the widest range of counter-illicit financing information sharing by financial institutions. This should include enabling compliance teams from different financial institutions to share information while working in common groups for purposes of mapping illicit financing networks. Such work could be facilitated by FinCEN and other investigative authorities, whose participation may require amending Section 314(a). This Committee should work with FinCEN to explore whether additional legislative authority is needed to advance these ideas and others to facilitate more effective information sharing by financial institutions in uncovering illicit financing networks.

Support Treasury Rulemaking under the BSA

(i) Support the issuance of Treasury's Proposed Rule on Customer Due Diligence (CDD), consistent with FATF global standards. Such action is required to address the systemic challenges posed by CDD practices that fall below global standards, particularly with respect to beneficial ownership. Treasury's proposed rule clarifying and strengthening CDD has incorporated and benefitted from exhaustive stakeholder comments collected through an outreach campaign unprecedented in the history of BSA rulemakings. Congressional support for Treasury's proposed rule may facilitate action by the Administration to finalize this rulemaking.

(ii) Support Treasury's consideration to extend AML/CFT preventive measures to investment advisers, consistent with FATF global standards. Such action is required to help address the systemic challenges created by gaps in the financial system that are not covered by AML/CFT preventive measures. As Treasury has reported in the 2015 National Money Laundering Risk Assessment, as of April 2015, investment advisers registered with the SEC reported more than $66 trillion assets under management. The current lack of AML/CFT regulation over this sector creates a significant blind spot in our understanding of whose interests are represented by this $66 trillion of assets, substantially undermining financial transparency in our capital markets. This gap also puts broker-dealers and other covered capital market sectors in the unfair and difficult position of trying to manage illicit financing risks of the investment adviser sector they service.

Congressional support for Treasury's consideration to extend AML/CFT preventive measures to this sector may facilitate such action by the Administration.

(iii) Support Treasury's consideration to extend AML/CFT preventive measures to real estate agents, consistent with FATF global standards. Such action is required to help address the systemic challenges created by gaps in vulnerable industries that are not covered by AML/CFT preventive measures. The longstanding global vulnerability of the real estate industry to money laundering is well-known. For this reason, FATF global standards direct countries to extend AML/CFT preventive measures to real estate agents. Several recent cases and investigative reporting by the media have indicated that this vulnerability continues to be exploited in the United States, perhaps most prominently in New York City and Miami. Treasury has long considered extending AML/CFT preventive measures to this industry. Congressional support may facilitate such action by the Administration.

(iv) Support Treasury's consideration of lowering the recordkeeping and travel rule thresholds for funds transfers from $3000 to $1000, consistent with FATF global standards. Such action is required to enhance the transparency of lower value funds transfers consistently abused to structure illicit financing transactions. Treasury's 2015 National Money Laundering Risk Assessment provides the latest evidence of such continued abuse. Lowering the thresholds to $1000 would triple the costs and risks for illicit financing networks engaged in such structuring. Maintaining a threshold of $1000 would preserve a reasonable threshold well above the average value of cross-border remittances, thereby avoiding any potential collateral and exclusionary impact on remittance flows. Congressional support for Treasury's consideration to lower this threshold may facilitate such action by the Administration.

Provide Additional Resources Targeting Strategic Investments to Strengthen Financial Integrity

Despite the clear and growing importance of financial integrity to our CFT campaign, national and collective security, and economic stability, US authorities responsible for protecting and advancing our financial integrity are severely stretched. These authorities are literally the best in the world at what they do, and their success has led to the welcome expansion of the counter-illicit financing mission and the continued protection of the expanding financial system. To maintain our unparalleled success, our counter-illicit financing authorities require the resources needed to match this expanding mission.

The critical importance of financial transparency and the proven impact of targeted financial measures represent a compelling investment opportunity for Congress to achieve a high return with relatively marginal costs. The recommendations below target specific investments that could significantly enhance our financial integrity and expand

the ability of the United States to combat national security threats through financial action.

(i) Provide protected resources for Treasury to enhance examination and supervision of BSA-covered industries lacking a federal functional regulator. Such action is needed to address the systemic challenges posed by AML/CFT regulatory coverage of high risk or vulnerable sectors that lack a federal functional regulator. Through the creative efforts of FinCEN and the IRS described above, Treasury has strengthened oversight and supervision of the MSB sector. These efforts would be further strengthened by additional resources that could be used to support a targeted supervisory and examination function managed by FinCEN, in continued coordination with the IRS. Such additional resources would also strengthen FinCEN's ability to oversee and enforce implementation of AML/CFT preventive measures in other industries lacking a federal functional regulator – including insurance companies, dealers in precious metals and stones, and casinos. Finally, such additional resources will be further needed if Treasury extends AML/CFT preventive measures to real estate agents, as recommended above.

(ii) Provide protected resources for Treasury's IRS and the Asset Forfeiture and Money Laundering Section of the Department of Justice to enhance financial investigations of illicit financing networks. Such action is needed to strengthen the systematic pursuit of illicit financing networks by the criminal investigative and prosecutorial authorities that are best suited and trained to support this mission. Such dedicated resources should be protected from competing interests of tax investigations in the case of the IRS and forfeiture actions by AFMLS. Such interests are obviously central to the respective missions of the IRS and AFMLS and critical to the broader financial integrity mission. Nonetheless, these interests should not preclude strengthening the parallel and sustained development of units dedicated to pursuing or supporting criminal investigations of the most sophisticated and dangerous illicit financing networks.

(iii) Provide protected resources for Treasury to enhance targeting of primary money laundering concerns under Section 311 of the USA PATRIOT Act and targeting of illicit financing networks under IEEPA. Such action is needed to give Treasury the resources it requires to continue applying targeted financial measures against a growing range of criminal and national security threats. The clearly disruptive impact of these actions and the increased demand for additional action justify additional resources that match the Treasury's expanding role in combating threats to our financial integrity and national security.

(iv) Provide protected resources for Treasury to develop foreign capacity in critical allies to support the effective implementation of AML/CFT measures and the application of targeted financial measures. Such action is required to strengthen

the global commitment to financial integrity and the impact of Treasury's targeted financial measures against those who threaten our collective security and the integrity of the global financial system.

Other Steps

(v) Task the Congressional Research Service to conduct a study of cross-border information-sharing requirements and prohibitions that our financial institutions must meet. Such action is needed to better understand the information-sharing challenges that our financial institutions face in identifying and managing transnational illicit financing risks. Armed with a better understanding, Congress can work with the Administration to develop solutions that assist our financial institutions in sharing the information they need to protect the integrity of our financial system.

(vi) Support the work of the AML Task Force in coordinating and strengthening examination, supervision and enforcement of AML/CFT preventive measures and financial sanctions. Such support may be needed to underscore the importance of collaboration across Treasury, law enforcement and the regulatory community to harmonize expectations for industry in implementing an effective risk-based approach to managing illicit financing risks. Such support may also encourage the development of new ideas and mechanisms to strengthen the integrity of the financial system, including through possible amendments to existing authorities to better align AML/CFT preventive measures to the risks facing our financial system. The 2015 National Money Laundering and Terrorist Financing Risk Assessments provide an excellent opportunity to reinvigorate this work.

Conclusion

Once again, I am honored and humbled to testify before you today in support of those across our government and financial services industries who fight every day to protect our financial integrity. They are the best in the world in advancing this mission. Their continued success will require your ongoing support.

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

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

Washington, D.C.
June 24, 2015

Good morning Chairman Fitzpatrick, Ranking Member Lynch, and Members of the Task Force to Investigate Terrorism Finance. Thank you for taking on this crucial issue, and for the opportunity to testify today. I would like to share with you the perspective of state and local law enforcement on nontransparent beneficial ownership, and the ease with which criminals and terrorists can operate anonymously in our jurisdictions.

Because of my Office's location in a global financial capital, I have a responsibility to combat terrorism financing and other financial crime. For decades, my Office has conducted investigations that rely on financial tracing and analysis to root out these crimes, as well as money laundering, sanctions violations, human trafficking, cyber crime, and other frauds. Like many in white-collar law enforcement, our *modus operandi* is to "follow the money," which in most cases means issuing subpoenas for records from financial institutions, and pursing the leads that those records provide. But sometimes, those records lead nowhere.

I want to share an anecdote which should be shocking. Sadly, it is not. While I was preparing for my testimony here, an investigator in my office entered the phrase "incorporate Delaware company" into Google. She called an incorporation services vendor that appeared in her search results. Putting on her best accent, she stated that she lives in

France, that she wanted to incorporate a company in Delaware, but that she wished to remain anonymous because of "estate issues" in her country. She was told that this would not be a problem; a corporation could be set up in five minutes – she needed to provide only a name and e-mail address. This starkly demonstrates what my colleagues and I know all too well: criminals currently can and do make use of our lax incorporation procedures and the anonymity those procedures permit in order to carry out and conceal illicit conduct

On a near-daily basis we encounter a company or network of companies involved in suspicious activity, but we are unable to glean who is actually controlling and benefiting from those entities, and from their illicit activity. In other words, we can't identify the criminal. This is not because the entities are incorporated in an offshore tax haven like the Cayman Islands. That country actually collects beneficial ownership information. Often, that entity is incorporated in the United States – and it's incorporated in the United States precisely because we don't collect beneficial owner information. In this important way, a prosecutor sitting in the Cayman Islands is better positioned to root out terrorism finance in her own markets than I am in ours.

Too frequently, an anonymous incorporation record spells the end of the road for our investigations. And when we are able, with much time and effort, to overcome that obstacle, we often find that criminals have purposefully relied on our lax incorporation requirements.

Recently, for example, a New York County Grand Jury indicted eight individuals in a sprawling "pump-and-dump" securities fraud scheme in which stock promoters and company insiders reverse-merged private companies with no publicly traded securities into existing public shell companies. They concealed their control of the shell companies by using nominees to purchase them, and to hold the publicly traded shares in their names. But the

scheme's mastermind appears nowhere in the incorporation documents, and held none of the companies' shares in his name. As in so many of our cases, disguised beneficial ownership is precisely what enabled the scheme.

The perils of anonymous incorporation go well beyond securities fraud. In 2011, Viktor Bout was convicted in New York of conspiring to sell millions of dollars' worth of weapons to the FARC, an OFAC-designated terrorist organization. The weapons were to be used to kill Americans in Colombia. By that time, Bout had earned the moniker "the merchant of death" following years of orchestrating arms shipments into conflict zones. Bout was able to do business largely thanks to a sprawling network of shell companies that he and his associates established. When OFAC designated 30 entities involved in his network in 2005, ten of them were U.S. companies, incorporated in Delaware and Texas. One of those U.S. entities provided weapons to the Taliban. Bout maintained absolute control over these accounts, but no links to Bout could be found in the entities' incorporation documents.

Indeed, shell companies doing business in New York can be used to disguise the activities of entire foreign governments. In 2006, my Office was investigating the Alavi Foundation, a non-profit organization which owned a 60 percent stake in a 36-story office building in midtown Manhattan. The remaining 40 percent was owned by the Assa Corporation, a New York-incorporated entity, and by Assa Company Limited, which was incorporated in the Channel Islands.

We ultimately determined that the Assa entities were merely shells being used to disguise the building's actual owner, a bank called "Melli." Bank Melli, as you may be aware, is wholly owned by the government of Iran. It was designated by OFAC as a key financier to Iran's nuclear and ballistic missiles program, and as a banker to the country's Revolutionary

Guard and Quds force. The building generated substantial rental income, which was diverted to the shell entities, and from there, to Bank Melli.

My Office routinely collaborates with foreign law enforcement to incapacitate cross-border threats. Time and again, we find that our international partners are better situated to assist *us* in thwarting terrorism and financial crime, than vice versa. It is detrimental to these partnerships when we have to tell international law enforcement that we can't assist them in taking down U.S.-incorporated terroristic enterprises, because information about the owners of entities *formed in our states* is beyond our reach.

Some might ask what good it would do to require that companies identify beneficial owners on incorporation documents, because, without verification, someone who intends to use a company for illicit purposes can just lie on the documents. That may be the case, but from the perspective of law enforcement, there is an enormous difference between a document that does not require certain information to be provided, and a document that falsely reports required information. The most obvious distinction is that the latter can provide law enforcement with a criminal charge: In New York, it is a felony to file a false business record.

In addition, the provision of false information goes a long way towards establishing criminal intent. It is of course true that the overwhelming majority of those who form corporations in the United States do so for perfectly lawful and respectable purposes. Listing a beneficial owner will not prove problematic for those individuals; it is only those who harbor illicit aims who would intentionally provide false information.

My Office has long supported the Incorporation Transparency and Law Enforcement Assistance Act (the "Act"). In testimony before the United States Senate Committee on Homeland Security and Governmental Affairs on June 18, 2009, my

predecessor, District Attorney Robert Morgenthau, called the bill "a no-brainer." Citing investigations by our Office into boiler rooms, pump-and-dump stock schemes, illicit Iranian money movement, and a foreign bank accused of laundering millions of dollars in drug money through New York, he observed that "[g]oing back to the early 1990's . . . the criminal actors in all of these cases benefited from systems lacking transparency." The inescapable conclusion, he testified, is that "[s]ystems promoting opacity and secrecy are the best friend of the money launderer, the tax cheat, the fraudster, the corrupt politician, and indeed, the financier of networks of terror."

There can be no doubt that the status quo promotes opacity, as well as a race to the bottom among the states. Absent federal action, this status quo will not change. States generally do not act against financial self-interest, and incorporation fees provide an important stream of revenue. No state can be reasonably expected to raise its standards unilaterally. A uniform minimal standard would level the playing field and end this pernicious race to the bottom. Only federal action can make it so.

I am also confident that the Act adequately safeguards the privacy of beneficial owners. The bill focuses on ensuring that law enforcement officials with a valid subpoena or summons may access beneficial ownership information, and it explicitly permits states to restrict the provision of beneficial ownership information to persons other than law enforcement.

A simple requirement to identify beneficial owners on state incorporation forms would vastly improve the capacity of American law enforcement to attack terrorism finance, and disrupt terror plots.

Thank you for the opportunity to testify today.

http://www.nytimes.com/2015/06/25/us/tally-of-attacks-in-us-challenges-perceptions-of-top-terror-threat.html

Homegrown Extremists Tied to Deadlier Toll Than Jihadists in U.S. Since 9/11

By SCOTT SHANEJUNE 24, 2015

New York Times

WASHINGTON — In the 14 years since Al Qaeda carried out attacks on New York and the Pentagon, extremists have regularly executed smaller lethal assaults in the United States, explaining their motives in online manifestoes or social media rants.

But the breakdown of extremist ideologies behind those attacks may come as a surprise. Since Sept. 11, 2001, nearly twice as many people have been killed by white supremacists, antigovernment fanatics and other non-Muslim extremists than by radical Muslims: 48 have been killed by extremists who are not Muslim, including the recent mass killing in Charleston, S.C., compared with 26 by self-proclaimed jihadists, according to a count by New America, a Washington research center.

The slaying of nine African-Americans in a Charleston church last week, with an avowed white supremacist charged with their murders, was a particularly savage case.

But it is only the latest in a string of lethal attacks by people espousing racial hatred, hostility to government and theories such as those of the "sovereign citizen" movement, which denies the legitimacy of most statutory law. The assaults have taken the lives of police officers, members of racial or religious minorities and random civilians.

Non-Muslim extremists have carried out 19 such attacks since Sept. 11, according to the latest count, compiled by David Sterman, a New America program associate, and overseen by Peter Bergen, a terrorism expert. By comparison, seven lethal attacks by Islamic militants have taken place in the same period.

If such numbers are new to the public, they are familiar to police officers. A survey to be published this week asked 382 police and sheriff's departments nationwide to rank the three biggest threats from violent extremism in their jurisdiction. About 74 percent listed antigovernment violence, while 39 percent listed "Al Qaeda-inspired" violence, according to the researchers, Charles Kurzman of the University of North Carolina and David Schanzer of Duke University.

"Law enforcement agencies around the country have told us the threat from Muslim extremists is not as great as the threat from right-wing extremists," said Dr. Kurzman, whose study is to be published by the Triangle Center on Terrorism and Homeland Security and the Police Executive Research Forum.

John G. Horgan, who studies terrorism at the University of Massachusetts, Lowell, said the mismatch between public perceptions and actual cases had become steadily more obvious to scholars.

"There's an acceptance now of the idea that the threat from jihadi terrorism in the United States has been overblown," Dr. Horgan said. "And there's a belief that the threat of right-wing, antigovernment violence has been underestimated."

Counting terrorism cases is a subjective enterprise, relying on shifting definitions and judgment calls.

If terrorism is defined as ideological violence, for instance, should an attacker who has merely ranted about religion, politics or race be considered a terrorist? A man in Chapel Hill, N.C., who was charged with fatally shooting three young Muslim neighbors had posted angry critiques of religion, but he also had a history of outbursts over parking issues. (New America does not include this attack in its count.)

Likewise, what about mass killings in which no ideological motive is evident, such as those at a Colorado movie theater and a Connecticut elementary school in 2012? The criteria used by New America and most other research groups exclude such attacks, which have cost more lives than those clearly tied to ideology.

Some killings by non-Muslims that most experts would categorize as terrorism have drawn only fleeting news media coverage, never jelling in the public memory. But to revisit some of the episodes is to wonder why.

In 2012, a neo-Nazi named Wade Michael Page entered a Sikh temple in Wisconsin and opened fire, killing six people and seriously wounding three others. Mr. Page, who died at the scene, was a member of a white supremacist group called the Northern Hammerskins.

In another case, in June 2014, Jerad and Amanda Miller, a married couple with radical antigovernment views, entered a Las Vegas pizza restaurant and fatally shot two police officers who were eating lunch. On the bodies, they left a swastika, a flag inscribed with the slogan "Don't tread on me" and a note saying, "This is the start of the revolution." Then they killed a third person in a nearby Walmart.

And, as in the case of jihadist plots, there have been sobering close calls. In November 2014 in Austin, Tex., a man named Larry McQuilliams fired more than 100 rounds at government buildings that included the Police Headquarters and the Mexican Consulate. Remarkably, his shooting spree hit no one, and he was killed by an officer before he could try to detonate propane cylinders he drove to the scene.

Some Muslim advocates complain that when the perpetrator of an attack is not Muslim, news media commentators quickly focus on the question of mental illness. "With non-Muslims, the media bends over backward to identify some psychological traits that may have pushed them over the edge," said Abdul Cader Asmal, a retired physician and a longtime spokesman for

Muslims in Boston. "Whereas if it's a Muslim, the assumption is that they must have done it because of their religion."

On several occasions since President Obama took office, efforts by government agencies to conduct research on right-wing extremism have run into resistance from Republicans, who suspected an attempt to smear conservatives.

A 2009 report by the Department of Homeland Security, which warned that an ailing economy and the election of the first black president might prompt a violent reaction from white supremacists, was withdrawn in the face of conservative criticism. Its main author, Daryl Johnson, later accused the department of "gutting" its staffing for such research.

William Braniff, the executive director of the National Consortium for the Study of Terrorism and Responses to Terrorism at the University of Maryland, said the outsize fear of jihadist violence reflected memories of Sept. 11, the daunting scale of sectarian conflict overseas and wariness of a strain of Islam that seems alien to many Americans.

"We understand white supremacists," he said. "We don't really feel like we understand Al Qaeda, which seems too complex and foreign to grasp."

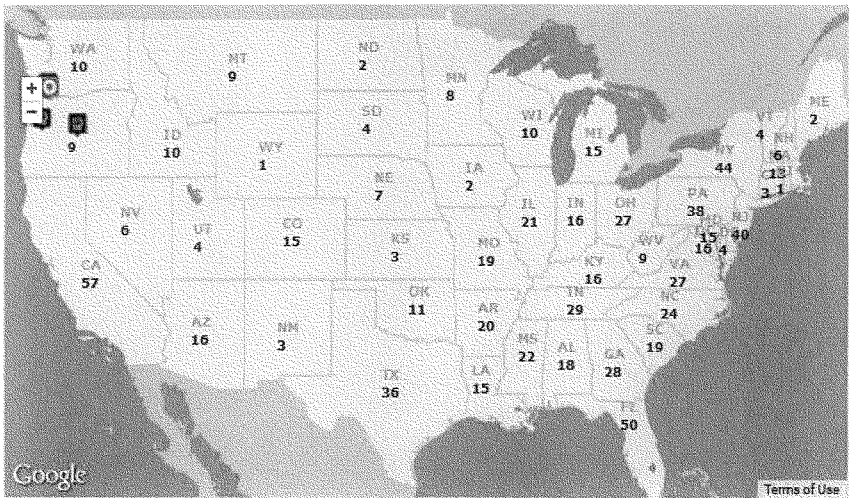
The contentious question of biased perceptions of terrorist threats dates back at least two decades, to the truck bombing that tore apart the federal building in Oklahoma City in April 1995. Some early news media speculation about the attack assumed that it had been carried out by Muslim militants. The arrest of Timothy J. McVeigh, an antigovernment extremist, quickly put an end to such theories.

The bombing, which killed 168 people, including 19 children, remains the second-deadliest terrorist attack in American history, though its toll was dwarfed by the roughly 3,000 killed on Sept 11.

"If there's one lesson we seem to have forgotten 20 years after Oklahoma City, it's that extremist violence comes in all shapes and sizes," said Dr. Horgan, the University of Massachusetts scholar. "And very often, it comes from someplace you're least suspecting."

Southern Poverty Law Center Hate Map

(Active U.S. Hate Groups by State)



John Carlson, Chief of Staff, Financial Services Information Sharing and Analysis Center, Response to Questions for the Record from Representative Keith Ellison

Evaluating the Security of the U.S. Financial Sector Hearing
Wednesday, June 24, 2015

Question 1: Domestic Terrorism Threats. As we prepare to bury the nine people killed at the Emanuel African Methodist Episcopal Church in Charleston, South Carolina, we know that we face internal terrorism threats. Domestic hate groups do engage in violent actions that kill people. In an article on June 24, 2015, *The New York Times* reports "Homegrown Radicals are More Deadly than Jihadis in the U.S."

"Since Sept. 11, 2001, nearly twice as many people have been killed by white supremacists, antigovernment fanatics and other non-Muslim extremists than by violent jihadists: 48 have been killed by extremists who are not Muslim, compared with 26 by self-proclaimed Muslim jihadists, according to a count by New America, a Washington research center."

Last week's murders were just one example of radicalization. In recent years, six people were murdered at a Sikh Temple in Wisconsin. There were three people killed at a Jewish Community Center and Assisted Living Facility in Kansas City.

How are financial institutions responding when Neo Nazi groups, white nationalist groups, the Klu Klux Klan, anti-government and other such violent hate groups try to access the financial system? Do financial institutions report such groups to national security agencies? Can you give us examples of when the financial sector was able to identify internal threats and work with law enforcement to prevent violence? What are we doing to track the flow of finances to these violent domestic hate groups? What agencies are charged with tracking the flow of funds through domestic terrorism groups? Are they adequately funded?

FS-ISAC Response: The role of the FS-ISAC is to distribute information to our members, pertaining to all hazards, including information related to both foreign and domestic threats. The FS-ISAC, however, is not a conduit for sharing account or personal information. Rather, as is required by federal law (e.g., Bank Secrecy Act, USA PATRIOT Act), individual financial institutions have a duty to report suspicious activity, such as known or suspected violations of law or transactional activities described in BSA/AML regulations, to the Financial Crimes Enforcement Network (FinCEN).

Question 2: Humanitarian Crisis in East Africa

Somalia – and other parts of East Africa face a humanitarian crisis. There are nearly no financial institutions willing to remit funds from the U.S. – or the U.K. or Australia –to Somalia. Are you concerned that the closure of these accounts may heighten the national security threat when people in Somalia, Sudan and other parts

of East Africa cannot get the resources they need to pay for food, school fees or business start-ups? How can we balance the need to curtail terrorism financing while simultaneously needing to ensure that the Somali population and other people in fragile nations have access to legitimate remittance channels?

FS-ISAC Response: The FS-ISAC is not involved in compliance with or policy advocacy relating to remittance or anti-terrorism laws and regulations. These questions are best addressed by the appropriate federal regulatory, law enforcement and national security agencies. As noted in my testimony, the FS-ISAC is a 501(c)6 nonprofit organization that focuses on sharing threat information; conducting coordinated contingency planning exercises; managing rapid response communications for both cyber and physical events, such Hurricane Sandy in 2012; and fostering collaborations with other key sectors and government agencies.

○