JEB HENSARLING, TX , CHAIRMAN

United States House of Representatives
Committee on Financial Services
2129 Rayburn House Office Building
Washington, D.C. 20515

MAXINE WATERS, CA, RANKING MEMBER

M E M O R A N D U M

To: Members of the Committee on Financial Services

From: FSC Majority and Minority Staff

Date: September 8, 2015

Subject: September 9, 2015, Task Force to Investigate Terrorism Financing hearing titled "Could America Do More? An Examination of U.S. Efforts to Stop the Financing of Terror"

The Task Force to Investigate Terrorism Financing will hold a hearing titled "Could America Do More? An Examination of U.S. Efforts to Stop the Financing of Terror" on Wednesday, September 9, 2015, at 10:00 a.m. in room 2128 of the Rayburn House Office Building. This will be a one-panel hearing with the following witnesses:

- Dr. Louise Shelley, Founder and Director, Terrorism, Transnational Crime, and Corruption Center, George Mason University
- Mr. Dan Larkin, Former FBI Unit Chief; Founder of the National Cyber Forensics & Training Alliance
- Mr. Scott Modell, Managing Director, The Rapidan Group
- Ms. Elizabeth Rosenberg, Senior Fellow and Director, Energy, Economics and Security Program, Center for a New American Security

Introduction

Terrorist financing is commonly described as a form of financial crime in which an individual or entity provides, stores, collects, and transports funds by any means, with the knowledge that such funds are intended to be used, in full or in part, to carry out acts of terrorism and sustain a terrorist organization, including the recruitment, retention, and training of terrorist group members.

While terrorist financing is likely only a small subset of financial crimes in terms of volume of transactions in the international financial system, it has long been a national security concern and became a renewed priority following the Al Qaeda attacks against the United States on September 11, 2001. In response to this threat, policymakers have sought to implement measures designed to halt the ability of terrorist groups to raise, move, and use funds.

Threats to the U.S. Financial System

Drawing on 2013 guidance produced by the Financial Action Task Force (FATF), an inter-governmental organization that promotes global anti-money laundering and counter-terrorist financing standards, the U.S. government issued two national risk assessments in June 2015, one on terrorist financing and another on money laundering. These documents update and add to a money laundering threat assessment issued a decade ago by the George W. Bush Administration. A June 2015 Task Force hearing also addressed the issue of U.S. financial sector security.[1]

According to the Treasury Department's June 2015 *National Terrorist Financing Risk Assessment*, the United States continues to face a "residual" risk of exposure to terrorist financing threats, due largely to the size and scope of international transactions that flow through the U.S. financial system. Terrorist financiers use various criminal schemes to fundraise in the United States, including through the charitable sector. Social media and other online communication platforms have provided financiers with new methods to solicit funds and recruits. Other emerging fundraising techniques involve the use of cybercrime and identity theft schemes.

The *National Terrorist Financing Risk Assessment* further concludes that terrorist groups continue to move funds through and place funds in the U.S. financial system by exploiting correspondent banking relationships with foreign financial institutions, conspiring with complicit money service business employees in the United States, and using unlicensed money transmitters to send funds abroad. Bulk cash smuggling continues to be a favored method of moving funds across U.S. borders. New payment systems may also be exploited by terrorists to move and place funds in the international financial system.

The *National Money Laundering Risk Assessment* notes that the underlying vulnerabilities within the U.S. financial system today "remain largely the same as those identified in 2005." Major vulnerabilities include the unreported use and movement of cash and monetary

[1] Task Force to Investigate Terrorism Financing, hearing on "Evaluating the Security of the U.S. Financial Sector," June 24, 2015.

instruments below record-keeping and reporting thresholds, challenges with implementing customer due diligence requirements and other anti-money laundering compliance deficiencies, use of shell companies to obfuscate beneficial ownership, and complicity of merchants and financial institutions to facilitate illicit transactions. Criminal proceeds annually generate an estimated $300 billion that are in turn laundered through the international financial system, according to the Risk Assessment. Most of these proceeds are derived from fraud- and drug trafficking-related crimes.

FATF-Designated High-Risk and Non-Cooperative Jurisdictions and U.S. Guidance

Three times each year, FATF's International Cooperation Review Group (ICRG) evaluates jurisdictions around the world for anti-money laundering and counter-financing of terrorism (AML/CFT) deficiencies. To protect the international financial system from those with the most concerning AML/CFT deficiencies, FATF recommends that all jurisdictions "apply effective counter-measures." The results of the most recent review were released on June 26, 2015, identifying 17 countries of concern.[2]

Jurisdictions that have strategic AML/CFT deficiencies and to which counter-measures apply: Iran and North Korea

Jurisdictions with strategic AML/CFT deficiencies that have not made improvements: Algeria and Burma

Jurisdictions with strategic AML/CFT deficiencies that have made political commitments to improve: Afghanistan, Angola, Bosnia and Herzegovina, Ecuador, Guyana, Laos, Panama, Papua New Guinea, Sudan, Syria, Uganda, Yemen

Jurisdictions with strategic AML/CFT deficiencies that are not making sufficient progress: Iraq

In response to FATF's ICRG review, the U.S. Department of the Treasury's Financial Crimes Enforcement Network (FinCEN) issued an advisory on July 20, 2015 that reminded financial institutions of the counter-measures in place against Iran and North Korea, including a broad array of U.S. and U.N. sanctions programs.[3] With respect to Algeria and Burma, FinCEN advised financial institutions to apply enhanced due diligence procedures when maintaining correspondent accounts for foreign banks operating under banking licenses issued by those countries. For all other listed countries, FinCEN advised financial institutions to ensure compliance with general due diligence obligations and, if appropriate, enhanced policies, procedures, and controls to detect and report suspected money laundering activity.

Global Terrorist Fundraising Sources

In the Task Force's first congressional hearing in April 2015, witnesses testified to the diversity and scope of today's terrorist financing threat, which has evolved since the Al Qaeda terrorist attacks of September 11, 2001, becoming more varied and localized.[4] Common methods for terrorist organizations to raise funds can include a combination of state sponsors, private donors, and licit and illicit revenue streams.

State Sponsors. Although fewer countries are identified today as state sponsors of international terrorism compared to during the Cold War era, overt and covert government sponsors reportedly remain active. Since 1984, for example, the State Department's has identified Iran as providing support to multiple terrorist groups (e.g., Palestinian terrorist groups in Gaza, including Hamas; Lebanese Hezbollah; various groups in Iraq and throughout the Middle East, including Iraqi Shia militias such at Kata'ib Hizballah; as well as through the Islamic Revolutionary Guard Corps-Qods Force). The issue of Iran's role in terrorist financing was featured in a July 2015 Task Force hearing.[5] Other State

[2] Financial Action Task Force, High-Risk and Non-Cooperative Jurisdictions, http://www.fatf-gafi.org/topics/high-riskandnon-cooperativejurisdictions/.

[3] Financial Crimes Enforcement Network, FIN-2015-A002, July 20, 2015.

[4] See for example prepared statement of Juan C. Zarate for a hearing held by the Task Force to Investigate Terrorism Financing, April 22, 2015. See also H. Hrg. 112-93.

[5] Task Force to Investigate Terrorism Financing, hearing on "The Iran Nuclear Deal and its Impact on Terrorist

Department-listed state sponsors of international terrorism include Sudan, designated as such since 1993, and Syria, designated since 1979.[6]

Private Donors. Private donors may include both a core group of wealthy individuals who are sympathetic to certain terrorist group goals as well as a broader network of local and diaspora community members who may or may not be aware that their donations are diverted for use by terrorist groups. According to the Obama Administration's 2011 *National Strategy for Counterterrorism*, Al Qaeda's main sources of financial support were wealthy private donors and charity organizations in the Arabian Peninsula.[7] The June 2015 *National Terrorist Financing Risk Assessment* identified Kuwait and Qatar as particularly permissive environments for donor-driven terrorist financing. Such financial support in turn flows from the region to Al Qaeda's affiliates and adherents around the world.

Self-Generated Profits. Sources of terrorist funds may include the proceeds of legitimate businesses, non-profit organizations, as well as illicit activities, such as drug trafficking, kidnapping for ransom, and extortion. In congressional testimony from February 2015, the Director of National Intelligence (DNI) James Clapper identified terrorism and transnational organized crime as among the top eight global threats to U.S. national security.[8] According to DNI Clapper, both terrorist and transnational criminal groups thrive in highly insecure regions of the world, with terrorist groups contributing to regional instability and internal conflict, while transnational organized crime groups exploit these environments for financial gain and corruptive influence. The February 2015 *National Security Strategy* echoed this concept of terrorism, crime, and corruption representing mutually reinforcing and interconnected threats—as did a May 2015 Task Force hearing on the financial implications of this nexus threat.[9]

Methods of Moving Terrorist Proceeds

Multiple methods for hiding and transporting terrorist funds exist. Despite regulatory controls and legal prohibitions, terrorists have exploited the international financial system through the following means: vulnerable non-financial businesses and professions, including charities, lawyers, accountants, and casinos; informal value transfer systems; and international trade systems. Selected examples include the following.

Financial Institutions. Terrorist organizations have used banks and non-bank financial institutions, such as currency exchange houses and other money services businesses, to store and move funds. Terrorists, including the 9/11 hijackers, have reportedly opened personal checking accounts, deposited and withdrawn cash, conducted international wire transfers, used travelers checks, and accumulated transactions on conventional credit

---

Financing," July 22, 2015.

[6] State Department, *2014 Country Reports on Terrorism*, June 2015.

[7] Obama Administration, *National Strategy for Counterterrorism*, June 2011.

[8] James Clapper, Director of the Office of National Intelligence, *Worldwide Threat Assessment of the U.S. Intelligence Community,* statement for the record, U.S. Senate, Committee on Armed Services, February 26, 2015.

[9] White House, Administration of President Barack Obama, *National Security Strategy*, February 6, 2015; Task Force to Investigate Terrorism Financing, hearing on "A Dangerous Nexus: Terrorism, Crime, and Corruption," May 21, 2015.

cards.[10] According to the June 2015 *National Terrorist Financing Risk Assessment*, foreign correspondent banking presents a particular challenge; in cases where insufficient customer due diligence safeguards were not in place, foreign banks with known links to terrorist organizations or terrorist financing have gained access to the U.S. financial system.

Informal and Unlicensed Value Transfer Mechanisms. Beyond the formal financial sector, unregulated mechanisms exist to anonymously transfer funds internationally. One such mechanism includes unregulated *hawala* transfers, which were reportedly used to facilitate the May 2010 attempted car bombing in New York City's Times Square and other previous terrorist activities.[11] According to the June 2015 *National Money Laundering Risk Assessment*, suspicious activity associated with informal money transmitters involve countries in the Middle East, particularly the United Arab Emirates, Yemen, and Iran, as well as in Latin America, including Venezuela, Argentina, and Mexico.

Charities. Charitable organizations are attractive for terrorist financing because of their presence in distressed parts of the world where terrorists often operate. Such organizations may be exploited as a source of income or as a cover for moving funds internationally in a nontransparent way. Although some donors may be sympathetic to radical causes, others are unaware that their funds may be clandestinely diverted for non-legitimate purposes. One such charity alleged to have been exploited by Al Qaeda and used to funnel funds to Chechen rebels includes the now-defunct, Saudi-based Al Haramain Islamic Foundation.[12] More recently, the June 2015 *National Terrorist Financing Risk Assessment* reported an emerging trend in which financiers solicit funds under the auspices of a charity or charitable cause with no connections to a charitable organization registered and recognized by the U.S. government.

Bulk Cash Movements. Another mechanism used to bypass the formal financial sector involves courier-facilitated transport of bulk cash or substitutes for cash, including gold or precious stones, often undeclared at ports of entry. According to the National Commission

[10] John Roth, Douglas Greenburg, and Serena Wille, *Monograph on Terrorist Financing*, National Commission on Terrorist Attacks Upon the United States (9/11 Commission), Staff Report to the Commission, Washington, DC, 2004.

[11] *Hawala* refers to an informal method for transferring funds that is commonly used in parts of the Middle East and South Asia where the formal banking system has limited presence. A *hawala* transfer typically involves a network of trusted money brokers, or *hawaladars*, who rely on each other to accept and disburse funds to third-party clients on their behalf. Settlement of account balances among *hawaladars* takes place subsequently, but not necessarily through bank and non-bank financial institutions. Such informal value transfer systems are often preferred because of their perceived quickness, reliability, and lower cost. Unregulated *hawala* systems, however, are perceived by government authorities as lacking sufficient transparency and investigations have revealed that they are vulnerable to abuse by terrorist groups. See U.S. Department of Justice, "Pakistani Man Sentenced on Unlicensed Money Transmitting Charges and Immigration Fraud," press release, April 12, 2011 and U.S. Department of the Treasury, Financial Crimes Enforcement Network (FinCEN), "Informal Value Transfer Systems," Advisory, FIN-2010-A011, September 1, 2010.

[12] Use of charities to raise funds for terrorist groups is not new. In the 1970s, for example, the Irish-American diaspora reportedly provided between $3 million and $5 million for the Irish Republican Army (IRA) through the purported charitable organization Irish Northern Aid Committee (NORAID). Daniel Byman, *Deadly Connections: States that Sponsor Terrorism* (New York: Cambridge University Press, 2005) and Roth, Greenburg, and Wille (2004).

on Terrorist Attacks Upon the United States (9/11 Commission), Al Qaeda regularly used couriers, recruited internally within the organization, to physically transport cash. Cross-border movements of Al Qaeda cash, upward of $1 million, have been reported.[13] For the 9/11 plot, Khalid Sheikh Mohammad reportedly couriered $120,000 to a contact in Dubai. The June 2015 *National Terrorist Financing Risk Assessment* concluded that cash smuggling will continue to be used as a means to move funds by a variety of terrorist organizations, including Al Qaeda and its affiliates, the Islamic State (ISIS or ISIL), Al Shabaab, Hezbollah, and the Revolutionary Armed Forces of Colombia (FARC).

Trade-Based Money Laundering (TBML). Trade-based money laundering involves the use of trade transactions to disguise the origin of illicit funds and move value internationally through the import or export of merchandise. TBML schemes vary in sophistication, but a simple example may involve the under- or over-invoicing of the price, quantity, or value of goods in a trade transaction. In 2011, U.S. officials alleged that Hezbollah was involved in a TBML scheme involving the laundering of cocaine proceeds from South America through the sale of used cars shipped and resold in West Africa.[14] The June 2015 *National Money Laundering Risk Assessment* notes that TBML is both a particularly difficult form of money laundering to investigate because it involves complicit merchants and also that it "can have a more destructive impact on legitimate commerce than other money laundering schemes." Illicit actors may dump imported goods at below-market prices to expedite the money laundering process, leaving legitimate businesses at a competitive disadvantage. Governments are also affected by lost tax revenue and customs duties on undervalued and fraudulently imported products.

Cyber Threats and Illicit Actors

In February 2015 congressional testimony on the U.S. intelligence community's assessment of worldwide threats, DNI Clapper highlighted cyber threats as a concern for U.S. national and economic security. According to Clapper, cyber threats are "increasing in frequency, scale, sophistication, and severity of impact."[15] A variety of actors, including terrorist organizations, nation states, ideological-driven criminals, and financially motivated entities, have, or are pursuing, cyber-capabilities that would allow them to finance their organization's operations and/or threaten the U.S. financial sector.

With respect to terrorists, Clapper stated in the same February 2015 congressional testimony that such actors would "continue to experiment with hacking" and could ultimately "develop more advanced capabilities." Additionally, he noted that "sympathizers will probably conduct low-level cyber attacks on behalf of terrorist groups and attract attention of the media, which might exaggerate the capabilities and threat posed by these actors." In remarks to the Aspen Security Forum in July 2015, FBI Director James Comey noted that the Bureau considered cyber threats by terrorists a "small but potentially growing problem"—and one that particularly piqued the interest of groups that have otherwise been thwarted in infiltrating or recruiting followers in the United States.[16]

[13] Roth, Greenburg, and Wille (2004).

[14] Financial Crimes Enforcement Network, U.S. Department of the Treasury, "Finding That the Lebanese Canadian Bank SAL Is a Financial Institution of Primary Money Laundering Concern," 76 *Federal Register* 33, February 17, 2011; U.S. Congress, House Committee on the Judiciary, Subcommittee on Crime, Terrorism, and Homeland Security, *Combating Transnational Organized Crime: International Money Laundering As A Threat To Our Financial Systems*, 112th Cong., 2nd sess., February 8, 2012, Serial No. 112-86 (Washington: GPO, 2012).

[15] Prepared statement of Director of National Intelligence James R. Clapper for a Senate Armed Services Committee hearing on the "Worldwide Threat Assessment of the U.S. Intelligence Community," February 26, 2015.

[16] Damian Paletta, "FBI Director Sees Increasing Terrorist Interest in Cyberattacks Against U.S.," *Wall Street Journal*, July 22, 2015.

The U.S. financial services business community appears to be a prime target of such cyber threats, variously attracting illicit cyber actors seeking access to funds, personally identifiable information, and client intellectual property.[17] During the 2012-2013 time period, the U.S. financial sector sustained one of the largest distributed denial of service (DDOS) attacks reportedly perpetrated by Iranian actors. Iranian actors were also implicated in the February 2014 cyber attack on the Las Vegas Sands casino company. Russia-based hackers were reportedly behind the 2014 data breaches of JP Morgan Chase & Co. and several other financial companies. North Korea has also been implicated in a 2013 hacking of several South Korean banks and media outlets.

Policy Responses in Historical Perspective

The foundations of contemporary U.S. policy to combat terrorist financing are grounded in anti-money laundering and counterterrorism policies that date back to the 1970s. The cornerstone of contemporary requirements for U.S. financial institutions to detect and report on suspicious transactions indicative of large-scale money laundering and criminal activities stems from the Bank Secrecy Act of 1970. Designations and prohibitions against state sponsors of terrorism and foreign terrorist organizations (FTOs) emerged in the late 1970s and evolved through the 1990s to include statutes that criminalized "material support" to terrorists and designated terrorist organizations (18 U.S.C. 2339A and 2339B; enacted in 1994 and 1996, respectively) and established targeted financial sanctions against FTOs and terrorist groups that were disrupting the Middle East Peace Process (Antiterrorism and Effective Death Penalty Act of 1996 and Executive Order 12947). The United Nations Security Council also mirrored U.S. policy in 1999, when it adopted Resolution 1267, to require U.N. member states to impose financial sanctions on the Taliban for providing support and sanctuary to Al Qaeda.

9/11 Commission Assessments

In reviewing the status of counterterrorism efforts prior to the Al Qaeda attacks on the United States on September 11, 2001, the 9/11 Commission concluded in a staff monograph devoted specifically to terrorist financing that U.S. and international efforts to target terrorist financiers and transnational funding flows were relatively weak.[18] The 9/11 Commission found efforts to deter financing were not a priority for domestic or international intelligence collection and lacked interagency and strategic planning and coordination. The existing statutes criminalizing material support for terrorists were reportedly rarely used to prosecute terrorist financing cases. Internationally, the 9/11 Commission reported that there was little emphasis on the enforcement and implementation of UNSCR 1267. Moreover, prior to 9/11, the United States had not ratified 1999 International Convention for the Suppression of the Financing of Terrorism.

As Al Qaeda plotted its attacks on the United States in 2001, the group relied on a wide range of methods to raise and transfer funds to its membership worldwide, according to the 9/11 Commission. Major sources of fundraising included wealthy private donors from Gulf countries in the Middle East and the diversion of funds from Islamic charitable organizations. Funds transfers involved a combination of formal financial sector

[17] See for example the House Financial Services Committee Oversight and Investigations Subcommittee hearing on "A Global Perspective on Cyber Threats," June 16, 2015.
[18] Roth, Greenburg, and Wille (2004).

mechanisms, informal value transfer mechanisms (e.g., *hawala*), and bulk cash movements involving trusted couriers. According to the 9/11 Commission, some $300,000 of the overall $400,000-$500,000 cost of the 9/11 attacks passed through U.S. bank accounts. The hijackers directly involved in the 9/11 attacks regularly deposited money into U.S. accounts through overseas wire transfers, cash deposits, and foreign travelers checks. They accessed such funds in the United States through conventional ATM withdrawals and credit card transactions.

Notably, the 9/11 Commission emphasized that the existing financial regulatory framework for anti-money laundering did not fail in 2001, as it was designed to detect and flag anomalous transactions more often associated with international drug trafficking and large-scale financial fraud rather than the routine-looking transactions conducted by the 9/11 hijackers.

9/11 Aftermath

Terrorist financing emerged as one of the key counterterrorism policy issues addressed during the immediate aftermath of Al Qaeda's September 2001 attacks. As the 9/11 Commission stated: "It is common to say the world has changed since September 11, 2001, and this conclusion is particularly apt in describing U.S. counterterrorist efforts regarding financing...."[19]

Immediately following 9/11, departments, bureaus, and agencies throughout the U.S. government sought to enhance intra- and inter-agency coordination on terrorist financing issues. The FBI established the Terrorism Financing Operations Section (TFOS) with its Counterterrorism Division to coordinate and centralize its efforts to track the financial underpinning of terrorist activity. The National Security Council (NSC) established the interagency Terrorist Financing Working Group (TFWG) in 2001 to coordinate the interagency delivery of training and technical assistance to combat terrorist financing, chaired by the State Department. In subsequent years, in the context of a changing mission brought on by the creation of the Department of Homeland Security (DHS) and an enhanced national security role, the Treasury Department underwent several institutional changes that emphasized counterterrorism finance.[20]

On September 23, 2001, President George W. Bush issued Executive Order 13224, blocking property and prohibiting transactions with persons who commit, threaten to commit, or support terrorism. In his public remarks on issuing EO 13224, President Bush explained: "Today, we have launched a strike on the financial foundation of the global terror network....

[19] Id.

[20] These changes culminated in 2004 with the establishment of the Office of Terrorism and Financial Intelligence (TFI) with a mission to marshal all of the Treasury Department's policy, enforcement, regulatory, and intelligence functions under the leadership of an Under Secretary-level office. Treasury's TFI, the Department of Justice's DEA, and the Department of Defense (DOD) also began establishing foreign-deployed "threat finance cells" as an interagency mechanism to collect, analyze, and act on financial intelligence related to the financial flows and transactions of priority insurgent and terrorist actors. The first such threat finance cell was established in 2005 in Iraq and the second in 2008 in Afghanistan. The Afghan Threat Finance Cell (ATFC), for example, was reportedly instrumental in discovering the illicit hawala-related financial activities of the New Ansari Exchange.

We have developed the international financial equivalent of law enforcement's 'Most Wanted' list. And it puts the financial world on notice.... Money is the lifeblood of terrorist operations. Today, we're asking the world to stop payment."[21]

In addition to redoubling efforts to use existing authorities and enforce existing regulations, Congress took additional actions following 9/11 through the enactment of several public laws, including the:

International Money Laundering Abatement and Anti-Terrorist Financing Act of 2001 (Title III of the USA PATRIOT Act, P.L. 107-56);

Suppression of the Financing of Terrorism Convention Implementation Act of 2002 (Title II of P.L. 107-197);

Intelligence Authorization Act for Fiscal Year 2004 (P.L. 108-177);

Intelligence Reform and Terrorism Prevention Act of 2004 (P.L. 108-458);

Combating Terrorism Financing Act of 2005 (Title IV of P.L. 109-177); and

Implementing Recommendations of 9/11 Commission Act of 2007 (P.L. 110-53).

In November 2001, the U.S. Senate also approved the 1999 International Convention for the Suppression of the Financing of Terrorism for ratification.[22] This treaty was intended to require the United States and other States Parties to criminalize terrorist financing and commit to international cooperation for the extradition and prosecution of suspects. In order for the United States to fulfill its obligations under this treaty, Congress enacted the Suppression of the Financing of Terrorism Convention Implementation Act of 2002 (Title II of P.L. 107-197).

Office of Terrorism and Financial Intelligence (TFI)

Subsequent congressional efforts to enhance U.S. efforts to combat threat finance included the establishment within the Treasury Department of the Office of Terrorism and Financial Intelligence (TFI) (P.L. 108-447), which leverages a combination of financial policy, enforcement, and intelligence capabilities to fulfill its mission of protecting the financial system "against illicit use and combating rogue nations, terrorist facilitators, weapons of mass destruction (WMD) proliferators, money launderers, drug kingpins, and other national security threats."[23]

Bureaus and offices within TFI include the Office of Terrorist Financing and Financial Crimes (TFFC), the Financial Crimes Enforcement Network (FinCEN), the Office of Foreign Assets Control (OFAC), and the Office of Intelligence and Analysis (OIA)—each of which

[21] President George W. Bush, *President Freezes Terrorists' Assets*, Remarks in the Rose Garden, Washington, DC, September 24, 2001.
[22] U.S. Congress, Senate, *Anti-Terrorism Conventions*, 107th Cong., 1st sess., November 27, 2001, Exec.Rpt. 107-2 (Washington: GPO, 2001).
[23] U.S. Department of the Treasury, *Terrorism and Financial Intelligence*, http://www.treasury.gov/about/organizational-structure/offices/Pages/Office-of-Terrorism-and-Financial-Intelligence.aspx.

have contributed to U.S. efforts to combat threats related to crime, terrorism, and corruption.

FinCEN, for example, has administered a procedure, authorized pursuant to the USA PATRIOT Act and popularly known as Section 311, to apply enhanced regulatory requirements, called "special measures," against designated jurisdictions, financial institutions, or international transactions deemed to be of "primary money laundering concern." Among the jurisdictional factors that can be considered when applying Section 311 measures, are "evidence that organized criminal groups, international terrorists, or both, have transacted business in that jurisdiction" as well as "the extent to which that jurisdiction is characterized by high levels of official or institutional corruption."

OFAC administers multiple sanctions programs to block transactions and freeze assets within U.S. jurisdiction of specified foreign terrorist, criminal, and political entities, including specially designated individuals and nation states. Authorities for OFAC to designate such entities are derived from executive order and legislative statutes, which include the International Emergency Economic Powers Act (IEEPA), the Antiterrorism and Effective Death Penalty Act of 1996 (AEDPA), and the Foreign Narcotics Kingpin Designation Act.

TFFC is the policy development and outreach office for TFI, which, among other priorities, leads the U.S. delegation to FATF.[24] OIA, which was established by the Intelligence Authorization Act for Fiscal Year 2004 (P.L. 108-177), contributes all-source financial threat assessments and products as a formal member of the U.S. Intelligence Community. Its analysts have been central in interagency efforts such as the Afghanistan Threat Finance Cell (ATFC) as well as its predecessor, the Iraq Threat Finance Cell (ITFC).

Selected Issues

As the House Financial Services Committee Task Force to Investigate Terrorism Financing conducts its fifth hearing in 2015 examining U.S. efforts to combat the financing of terrorism, several ongoing policy issues facing the 114th Congress include:

Information sharing. Some have called for congressional action to improve and expand existing information sharing tools between financial institutions and government authorities and among financial institutions in cases of suspected money laundering and terrorist financing—including changes to the scope of liability safe harbors and the types of information that may be shared. In testimony before the Task Force, Chip Poncy of the Foundation for Defense of Democracies included gaps in information sharing as a "systemic challenge to financial transparency." Similar policy concerns also affect financial institutions with respect to cyber threat-related information sharing. John Carlson of the Financial Services Information Sharing and Analysis Center also testified before the Task Force, noting the private

[24] The Intelligence Reform and Terrorism Prevention Act of 2004 (P.L. 108-458) authorized the Secretary of the Treasury, or the Secretary's designee, as the lead U.S. government official to the Financial Action Task Force.

sector's interests in enhanced cyber threat information sharing legislation that would provide a variety of liability and disclosure protections for sharing and receiving cyber threat information.

Beneficial ownership. According to a FATF-conducted mutual evaluation of the U.S. AML/CFT system in 2006, one of the few areas in which the United States was rated "non-compliant" with international AML/CFT standards involved information collection on beneficial ownership and control of legal entities. The risk of terrorist, criminals, and corrupt actors exploiting beneficial ownership information gaps in the United States to create and use shell companies for illicit purposes has long been a concern to Congress as well. Several witnesses at Task Force hearings have raised the issue, including New York County District Attorney Cyrus Vance, Jr.. For its part, the Obama Administration has also sought to address this issue through international commitments and proposed legislative and regulatory changes. The next FATF mutual evaluation of the United States is scheduled for 2016.

Islamic State. As the 114th Congress continues to consider and evaluate U.S. policy responses to address the Islamic State, a focus of concern may center on whether U.S. counterterrorist financing tools are capable of diminishing IS sources of funds. Key questions may include whether current U.S. efforts are effective and sufficiently resourced, or require new legislative authorities, to respond to the Islamic State's ability to accumulate and distribute funds. Although Congress has been active in evaluating U.S. policy responses and options to address the Islamic State, particularly the military response and prospects for congressional authorization for the use of military force, legislative proposals to stem the Islamic State's access to and use of funds have been limited. Many observers recognize that a strategy focused on counter-finance may weaken, but not destroy, the Islamic State. For its part, the Department of the Treasury has cautioned against expectations that efforts to combat the Islamic State's finances will bear fruit quickly.

Iran. Observers have cautioned that the July 2015 negotiated Iran nuclear deal, known as the Joint Comprehensive Plan of Action (JCPOA), could have implications for terrorist financing, a topic that was addressed in a recent Task Force hearing. Although proliferation-related sanctions relief pursuant to the JCPOA would leave in place existing terrorism-related sanctions against Iran, some remain concerned about the possibility that Iran may allocate more resources to terrorist financing as its economic prospects improve. Should the JCPOA be implemented, a potential challenge for the United States and the international financial services community would be how to ensure that the terrorist financing risks emanating from Iran are effectively mitigated.

Witness Biographies

Dr. Louise Shelley, Founder and Director, Terrorism, Transnational Crime, and Corruption Center, George Mason University

Dr. Louise Shelley is the Omer L. and Nancy Hirst Endowed Chair and a University Professor at George Mason University. She is in the School of Policy, Government, and International Affairs and directs the Terrorism, Transnational Crime and Corruption Center (TraCCC) that she founded. She is a leading expert on the relationship among terrorism, organized crime and corruption as well as human trafficking, transnational crime and terrorism with a particular focus on the former Soviet Union. She also specializes in illicit financial flows and money laundering.

Dr. Shelley received her undergraduate degree cum laude from Cornell University in Penology and Russian literature. She holds an M.A. in Criminology from the University of Pennsylvania. She studied at the Law Faculty of Moscow State University on IREX and Fulbright Fellowships and holds a Ph.D. in Sociology from the University of Pennsylvania. She held a Fulbright and researched and taught on crime issues in Mexico. She has also taught on transnational crime in Italy. She is the recipient of the Guggenheim, NEH, IREX, Kennan Institute, and Fulbright Fellowships and received a MacArthur Grant to establish the Russian Organized Crime Study Centers and is now working on a MacArthur grant studying non-state actors and nuclear proliferation. In 1992, she received the Scholar-Teacher prize of American University, the top academic award of the university. .

Daniel Larkin, Former FBI Unit Chief; Founder of the National Cyber Forensics & Training Alliance

Mr. Larkin served in the FBI for more than 24 years and established the first Cyber Fusion Unit for the Federal Government, enabling Govt/Law Enforcement to effectively co-locate with Subject Matter Experts (SMEs) from industry & academia. This Unit substantially enhances resource sharing (personnel, technology & intelligence) to the mutual benefit of all participants. Private Sector partners include numerous financial services organizations, telecommunications, technology, and e-commerce. Law Enforcement partners include a growing list of Federal, State & Local agencies, as well as international investigators from more than a dozen countries.

Mr. Larkin also developed one of the first High Tech Crime Task Forces in the United States. This unique collaboration of assets also led to the development of the first national Public/Private Alliance to identify and combat cyber crime, known as the National Cyber Forensics & Training Alliance (NCFTA). Mr. Larkin also co-authored the FBI National Cyber Crime strategy in 2002.

Mr. Scott Modell, Managing Director, The Rapidan Group

Scott Modell is the Managing Director of The Rapidan Group. Mr. Model is an uncommonly talented and seasoned expert on Iran and the broader Middle East and offers unparalleled insight into geopolitical and energy related developments and trends in that region, as well as Latin America and Europe. He is a highly decorated former Central Intelligence Agency officer who served for 13 years in the Directorate of Operations, with five tours conducting Iranian operations in Latin America, Western Europe, and the Middle East. He also participated in post 9-11 operations in Afghanistan, serving on the battlefields in the southern and southeastern regions of the country as a member of paramilitary counterterrorism teams composed of CIA officers and local Afghan forces. In addition to his Rapidan Group responsibilities, Scott is currently a Non-Resident Fellow at the Center for Strategic and International Studies focusing on security issues related to Iran and the Middle East and a senior advisor to U.S. Special Operations Command on Counter Threat Finance operations. Scott is fluent in Spanish, Farsi, and Portuguese, and received his M.A. from the Georgetown School of Foreign Service.

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

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

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

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

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