Statement of

Celina B. Realuyo*

Professor of Practice

William J. Perry Center for Hemispheric Defense Studies

at National Defense University

on

"Communicating, Cooperating and Collaborating through Public-Private Partnerships to Counter the Financing of Terrorism and Crime"

at a Hearing Entitled

"The Next Terrorist Financiers: Stopping Them Before They Start"

Before the Task Force to Investigate Terrorism Financing,

Committee on Financial Services,

U.S. House of Representatives

June 23, 2016

***** The views expressed in this testimony are my own and do not necessarily reflect the views of the William J. Perry Center for Hemispheric Defense Studies, National Defense University, or the Department of Defense.

Thank you Chairman Fitzpatrick, Vice Chairman Pittenger, Ranking Member Lynch, and members of the Task Force to Investigate Terrorism Financing for the opportunity to appear before this committee today to testify on U.S. efforts to combat the financing of terrorism and money laundering that threaten U.S. national security interests at home and abroad. Today we face a broad spectrum of security threats such as global terrorism, transnational organized crime, economic crises, cyber attacks, extreme natural disasters and revisionist states that have made national security more challenging than ever before. The complexity of these security threats, particularly from illicit networks, such as terrorists, criminals and proliferators, requires a multi-disciplinary approach to comprehend and counter them effectively.

The convergence of these illicit networks and the magnitude, velocity and violence associated with their illegal activities are overwhelming governments and threatening state sovereignty and our economy. Governments can no longer guarantee the security, prosperity, rule of law and governance that their people expect and deserve. Often, average citizens who "see something and say something" are the first to recognize anomalies and identify threats; they know their industries, workplaces and communities best. For these reasons, governments need to actively identify and engage partners in the private and civic sectors to better detect, dismantle and deter the bad actors that undermine our security, economy and society. By fostering more robust partnerships among the public, private and civic sectors of society, together, we can better counter the convergence of illicit networks in the U.S. and overseas.

Money serves as the lifeblood for any activity, licit or illicit; financing is the most critical of enablers for terrorism, crime and corruption. In the post-9/11 world, we have witnessed how "following the money trail" has enhanced our efforts to counter the threats around the world. Since international financial flows are not controlled or managed by governments, public-private partnerships with the many facets of the financial services industry are essential in combating threats to the international banking system, such as terrorist financing, money laundering, political corruption and cybercrime. Governments

no longer enjoy a monopoly on national security or the use of force as they did in the past; therefore, they need to adopt a "whole of society" approach to understand and address the evolving threats to our security and prosperity in this globalized world. In the 21st century, all sectors need to communicate, cooperate and collaborate (C^3) through public private partnerships (P^3) to counter the convergence of illicit networks and safeguard national security.

U.S. and Coalition Efforts to Counter the Islamic State in Syria and the Levant (ISIL)

Before elaborating on the importance of public-private sector collaborations to counter threat finance and protect the international financial system, let me provide a contextual update on U.S. and Coalition efforts to counter the financing of ISIL. ISIL is the most prominent example of the terror-crime convergence threatening Iraq, Syria and beyond. "Following the money trail" of ISIL has been instrumental in our understanding and planning for the detection, disruption and dismantling of ISIL and its support networks. The methodical use of the financial instrument of national power, through financial intelligence gathering and targeting key leadership and their critical assets, has degraded ISIL's revenue-generating abilities and its capacity to fund and sustain its criminalized caliphate.

As articulated by the White House, the U.S. has built a global coalition of over 60 partner nations with the goal of degrading and ultimately defeating ISIL. In November 2014, President Obama set forth a comprehensive strategy featuring nine lines of collective effort to counter ISIL:

1. Supporting Effective Governance in Iraq
2. Denying ISIL Safe-Haven
3. Building Partner Capacity
4. Enhancing Intelligence Collection on ISIL
5. Disrupting ISIL's Finances
6. Exposing ISIL's True Nature

7. Disrupting the Flow of Foreign Fighters
8. Protecting the Homeland
9. Humanitarian Support[1]

Since I last appeared before this committee in May 2015, we have witnessed progress on the military and financial fronts of the fight against ISIL. According to the State Department 2015 Country Reports on Terrorism, ISIL remains the greatest threat globally, maintaining a formidable force in Iraq and Syria, including a large number of foreign terrorist fighters. That said, ISIL's capacity and territorial control in Iraq and Syria reached a high point in spring 2015, but began to erode over the second half of the year. For example, at the end of 2015, 40 percent of the territory that ISIL controlled at the beginning of that year had been liberated. In Syria, local forces expelled ISIL fighters from several key cities along the routes connecting the two ISIL strongholds of Raqqa and Mosul, and reclaimed about 11 percent of the territory ISIL once controlled. These losses demonstrated the power of coordinated government action to mobilize against and confront terrorism.[2]

The loss of territory ISIL governs and controls in Iraq and Syria in 2015 also resulted in diminished funds available to it. ISIL relies heavily on extortion and the levying of "taxes" on local populations under its control, as well as oil smuggling, kidnap for ransom, looting, antiquities theft and smuggling, foreign donations and human trafficking. Coalition airstrikes targeted ISIL's energy infrastructure – modular refineries, petroleum storage tanks and crude oil collection points – as well as many millions that were literally stored in bulk cash storage sites. These airstrikes have significantly degraded ISIL's ability to generate revenue. The U.S. led this international effort,

---

[1] The White House, FACT SHEET: The Administration's Strategy to Counter the Islamic State of Iraq and the Levant (ISIL) and the Updated FY 2015 Overseas Contingency Operations Request, November 7, 2014, https://www.whitehouse.gov/the-press-office/2014/11/07/fact-sheet-administration-s-strategy-counter-islamic-state-iraq-and-leva

[2] U.S. State Department Country Reports on Terrorism 2015, Strategic Assessment, http://www.state.gov/j/ct/rls/crt/2015/257513.htm

including through the UN, to confront ISIL's oil smuggling and its antiquities dealing, delivering additional blows to its financial infrastructure.[3]

More recently, appearing before the Senate Armed Services Committee on April 28, 2016, Secretary of Defense Carter described the headway that the Coalition has made to counter ISIL on the military front through "Operation Inherent Resolve."[4] The United States has spent $6.4 billion on counter-IS military operations since August 8, 2014, with an average daily cost of $11.5 million.[5] Secretary Carter said: "We've seen results in targeting ISIL's leaders and finances. We're systematically eliminating ISIL's "cabinet," having taken out its so-called ministers of war and finance. We captured one of the principals of ISIL's chemical warfare enterprise, removed external plotters from the battlefield, and most recently took out the ISIL emir for southern Mosul, weakening ISIL's ranks there. And our attacks on ISIL's economic infrastructure – from oil wells and trucks to cash storage to ISIL's financial leaders – is putting a stranglehold on ISIL's ability to pay its fighters, undermining its ability to govern, and making it harder to attract new recruits.[6]

ISIL is on its heels in Iraq and Syria as the Iraqi armed forces seek to retake control of Fallujah and Mosul, key ISIL strongholds. The Fallujah offensive, which began May 22, follows a series of ISIL defeats in western Anbar province, a longtime Sunni Muslim stronghold and a bastion of support for anti-government militants since the U.S.-led invasion of Iraq in 2003. Iraqi government forces, backed by training, advice and air support from a U.S.-led international coalition, retook Ramadi in December 2015 and Hit four months later. After Fallujah, the northern city of Mosul is the last major

---

[3] *Ibid.*
[4] U.S. Department of Defense Operation Inherent Resolve website, http://www.defense.gov/home/features/2014/0814_iraq/
[5] U.S. Department of Defense, "Operation Inherent Resolve: Targeted Operations against ISIL Terrorists," http://www.defense.gov/News/Special-Reports/0814_Inherent-Resolve
[6] Secretary of Defense Testimony, Statement on Counter-ISIL Operations and U.S. Military Strategy in the Middle East before the Senate Armed Services Committee, As Delivered by Secretary of Defense Ash Carter, Washington, D.C., April 28, 2016 Secretary of Defense Ash Carter Testimony, http://www.defense.gov/News/Speeches/Speech-View/Article/744936/statement-on-counter-isil-operations-and-us-military-strategy-in-the-middle-eas

urban area in Iraq controlled by Islamic State that promises to be a fierce battle against the group.[7]

ISIL - An Adaptive Adversary

While the momentum of the counter-ISIL offensive by the Coalition looks promising on the military and financial fronts, ISIL is proving to be a very adaptive adversary and is expanding its reach well beyond Iraq and Syria. ISIL has a diversified spectrum of criminal and revenue-generating activities that provides it the flexibility to respond to Coalition attacks on its financial infrastructure. Terrorism experts Jean-Charles Brisard and Damien Martinez, in a May 2016 report at the Center for the Analysis of Terrorism, stated "despite the constant airstrikes on its oil infrastructure, ISIL still has a $2 billion empire; and it's making up lost revenue by squeezing the population under its control through raising taxes. ISIL's military defeat is not imminent. As things stand, ISIL economic collapse remains some way off in the mid-term."[8]

The report posits that ISIL made $2.4 billion in 2015, a $500 million drop from the center's revenue estimate the previous year. The main reason ISIL is still making billions is taxes. ISIL's extortion of the people trapped inside its territory in Iraq and Syria has skyrocketed from $360 million in 2014 to $800 million in 2015, according to researchers. According to the U.S. Treasury Department, the Coalition's effort to disrupt the ISIL's economy is working. "We are seeing progress... since late-2015, ISIL's production of oil has declined by about 30%. Their ability to generate revenue has been reduced by at least that much," Treasury said.[9] As oil revenues have declined, ISIL is becoming more reliant on extortion and taxation in the territories that it still occupies. Therefore, re-establishing control of those territories is essential to defeating ISIL militarily, financially, and psychologically.

---

[7] Ghassan Adnan and Asa Fitch, "Iraqi Counterterrorism Forces Enter Fallujah," *Wall Street Journal*, June 8, 2016, http://www.wsj.com/articles/iraqi-counterterrorism-forces-enter-fallujah-1465389277

[8] Jose Pagliery, "ISIS Makes Up for Lost Oil Cash with Rising Taxes and Fees," May 31, 2016, CNN.com, http://money.cnn.com/2016/05/31/news/isis-oil-taxes/

[9] *Ibid.*

ISIL's Influence Beyond Syria and Iraq

ISIL's claim to be a caliphate has raised concerns that its ambitions stretch well beyond Syria and Iraq. The tragic terrorist attacks in Paris on November 13, 2015 and the claimed downing of a Russian plane over the Sinai just weeks earlier demonstrate that ISIL's aspirations are global in nature. ISIL is thinking beyond the Middle East—and, increasingly, it is demonstrating capabilities to act beyond the region as well. Militant groups in Egypt, Nigeria, Pakistan, Afghanistan, Indonesia and the Philippines have taken up the ISIL's trappings and sworn allegiance to its leader, al-Baghdadi. According to the Heritage Foundation, in just two years—from fall 2013 to fall 2015—ISIS established a presence in at least 19 countries.[10]

Libya represents ISIL's new caliphate. According to the State Department, ISIL's branch in Libya was estimated to have up to 5,000 terrorist fighters. The group has seized territory that spans more than 150 miles of Mediterranean coastline between the cities of Tripoli and Benghazi. It also conducted attacks in Libya's oil crescent and in Sabratha, near the border with Tunisia. However, ISIL also suffered losses in Libya in confrontations with militia groups, in particular in the eastern Libyan city of Darnah.[11] The U.S. and its European allies are increasingly concerned about ISIL's expansion in North Africa, have intensified pressure on Libya's divided governments and factions to reconcile, and signaled they are considering expanding military operations there.[12]

The conflicts in Syria and Iraq have attracted foreign fighters by the thousands. Middle Eastern and Western intelligence agencies have raised concern that their citizens who have joined the fighting in Iraq and Syria will become radicalized and then use their

---

[10] Lisa Curtis, Luke Coffey, David Inserra, Daniel Kochis, Walter Lohman, Joshua Meservey, James Phillips and Robin Simcox, *Combatting the ISIS Foreign Fighter Pipeline: A Global Approach*, The Heritage Foundation, January 2016, http://www.heritage.org/research/reports/2016/01/combatting-the-isis-foreign-fighter-pipeline-a-global-approach

[11] U.S. State Department Country Reports on Terrorism 2015, Strategic Assessment, http://www.state.gov/j/ct/rls/crt/2015/257513.htm

[12] Zachary Laub, Online Writer/Editor, and Jonathan Masters, Deputy Editor, *CFR Backgrounder, The Islamic State*, Council on Foreign Relations, March 22, 2016, http://www.cfr.org/iraq/islamic-state/p14811

passports to carry out attacks in their home countries. Unfortunately, we have seen this to be the case in recent terror attacks in Paris and Brussels. U.S. Director of National Intelligence James Clapper estimated in February 2015 that more than thirteen thousand foreign fighters joined Sunni Arab antigovernment extremist groups, including the Islamic State, in Syria, and that more than 3,400 of more than twenty thousand foreign Sunni militants hailed from Western countries. (Estimates of the group's total forces range from around thirty thousand to more than a hundred thousand.)[13]

The influence of ISIL has reached U.S. homeland. In July 2015, FBI Director Comey estimated that upwards of 200 Americans have traveled or attempted to travel to Syria to fight alongside ISIL.[14] In addition to recruiting foreign fighters, ISIL has inspired homegrown terrorists responsible for the deadly December 2015 San Bernardino and more recently the June 12, 2016 Orlando attacks. Just days before the Orlando attack, FBI Director James Comey eerily spoke about the three prongs to the ISIL threat: the recruitment to travel, the recruitment to violence in place, and then what you saw a preview of in Brussels and in Paris — hardened fighters coming out, looking to kill people. Comey reiterated that the FBI has close to 1,000 open cases nationwide involving people at various stages of ISIL recruitment.[15] The Orlando attack at the Pulse nightclub left 49 dead and 53 wounded, representing the deadliest mass shooting in U.S. history. Omar Mateen, a self-radicalized 29-year old U.S. citizen of Afghan descent, who pledged allegiance to ISIL on a 911 call during the attack, perpetrated the terrorist act, according to the initial FBI investigation.[16]

The contemporary threat posed by ISIL to global security has been empowered by a dangerous convergence of terrorism and crime that generates significant income for the

---

[13] Zachary Laub, Online Writer/Editor, and Jonathan Masters, Deputy Editor, *CFR Backgrounder, The Islamic State*, Council on Foreign Relations, March 22, 2016, http://www.cfr.org/iraq/islamic-state/p14811

[14] Julian Hattem, "FBI: More than 200 Americans have tried to fight for ISIS, *The Hill*, July 8, 2015, http://thehill.com/policy/national-security/247256-more-than-200-americans-tried-to-fight-for-isis-fbi-says

[15] Associated Press, "FBI Director: No Decrease In Number Of US ISIS Cases," Minnesota CBS Local News, June 7, 2016, http://minnesota.cbslocal.com/2016/06/07/fbi-isis/

[16] Ralph Ellis, Ashley Fantz, Faith Karimi and Eliott C. McLaughlin, "Orlando shooting: 49 killed, shooter pledged ISIS allegiance," CNN.com, June 13, 2016, http://www.cnn.com/2016/06/12/us/orlando-nightclub-shooting/

group. The systematic practice of "taxation," oil smuggling, kidnapping for ransom, human trafficking, and antiquities looting across the territory it occupies provide vital resources for the group's military, financial, recruitment, and propaganda campaigns. Continued supply and demand for illicit goods and services, and ISIL control of the supply chains in these criminal markets, provide it with an ideal operating environment its illicit activities that now expands beyond Iraq and Syria. Neutralizing this synergy requires a global coalition that encompassing the public, private and civic sectors on a transnational level. While raising awareness of ISIL's brutal crimes like sexual slavery and antiquities trafficking can reduce demand, the most effective manner to counter it remains the military, financial, and ideological defeat of the ISIL and a reinstatement of control of the occupied territories in Iraq and Syria and beyond.[17]

Public-Private Sector Collaboration to Safeguard the International Financial System

Since the 1970's, the U.S. government recognized the need to work with the private sector to pursue financial crimes like fraud, tax evasion, and money laundering. Under the Bank Secrecy Act of 1970, or BSA for short, U.S. financial institutions are required to assist U.S. government agencies to detect and prevent money laundering. Specifically, the BSA requires banks to keep records of cash purchases, file reports of cash transactions exceeding $10,000, and report suspicious activity that might indicate money laundering, tax evasion, or other criminal activities.[18] Financial institutions are required to know their clients (and their clients' clients), monitor their transactions for anomalies, and report concerns to the authorities.

In the U.S., FinCEN (the Financial Crimes Enforcement Network) serves as the country's financial intelligence unit (FIU), collecting and analyzing suspicious transaction reports; FinCEN has counterparts globally, providing the opportunity for global cooperation. Once it came to light that Al Qaeda used the formal banking system to finance the 9/11 attacks, banks and other financial institutions, concerned with

[17] Celina B. Realuyo, "The ISIS Convergence," *American Foreign Policy Council Defense Dossier*, March 2016, HTTP://WWW.AFPC.ORG/FILES/DEFENSE_DOSSIER_MARCH_ISSUE_16.PDF
[18] U.S. Bank Secrecy Act, FinCEN website, http://www.fincen.gov/statutes_regs/bsa/

reputational risk, realized they had a new and vital task -- to detect and report possible cases of terrorist financing. Now bankers needed to understand and identify how terrorist groups raise, move, store, and use money and what vulnerabilities exist in banking system to prevent future cases of terrorist financing. Not only did the modes and rules change, but so did the forward-leaning posture of the industry which became more motivated to interact and share information with the government and fellow financial institutions.

U.S. Counterterrorism Financing and Anti-Money Laundering Efforts

The U.S. law enforcement and intelligence community works closely with officials at various financial institutions, many of whom have been vetted and hold an active security clearance, to investigate and prosecute specific cases of terrorist financing and money laundering. Increasingly, bank officials are former law enforcement agents or bank regulators. The financial sector has invested billions in human, technological, and financial resources to enhance their AML/CTF (anti-money laundering/counterterrorist financing) compliance capabilities. While these relationships between the public and private sectors have been quite productive, particularly in detecting Iranian sanctions violations, some financial institutions have expressed frustration regarding the lack of information flow from the government on the impact this cooperation has had on actual cases. Not knowing the details about the value of these submissions makes it harder to be compliant and misses the opportunity to fine-tune a company's internal capacity to identify violations and suspicious activity. The private sector continually calls for better two-way communications and more information to justify and effectively direct the immense investment in AML/CTF programs to the board and shareholders who require proof that the money was well spent.

There are many examples of successful venues through which private industry and government work together. In 2010, the Financial Intelligence and Information Sharing Working Group (FIIS WG) was established following the completion of a public-private partnership pilot project under the auspices of the Office of the Director of

National Intelligence's Office of Private Sector Partnerships. The original project's content aside, both the analysts and the business people involved found that the shared communication about threat-finance typologies and red flags was productive. To keep the dialogue going, the participants started a free-standing group which organically blossomed due to the information-sharing gaps in this area. While the group has no affiliation with the government, the FIIS WG is intended to provide experts in the financial services industry and the U.S. government with a forum to informally discuss relevant topics, including protection of critical financial infrastructure, prevention of fraud, and counterterrorist financing and money laundering.

FIIS WG meetings and the relationships formed at those events facilitate information flow and bridge cultural gaps between government and industry. The FIIS WG eventually found a home with the American Security Project, (a non-partisan public policy & research organization in Washington, D.C.) Its members include hundreds of representatives of both public and private sector entities, including regulatory, intelligence, defense, and law enforcement agencies, financial institutions, think tanks, consultancies, and academia.[19] The FIIS WG has become a peer-to-peer community of practice and useful forum to exchange knowledge and experience about red flags, trends, emerging financial technologies, new payment systems, virtual currencies, alternative value systems, and the threats and vulnerabilities that accompany them.

Besides the banks themselves, several trade associations and nongovernmental organizations have become actively involved in raising awareness, training, and educating the financial industry on the threats to the international financial system from financial crimes. One such example is ACAMS, the Association of Certified Anti-Money Laundering Specialists. It is the largest international membership organization dedicated to enhancing the knowledge, skills and expertise in AML/CTF (anti-money laundering and countering terrorist financing) and financial crime detection and prevention. Members represent various financial institutions, regulatory bodies, law enforcement

[19] American Security Project Threat Finance and Financial Intelligence website, http://www.americansecurityproject.org/asymmetric-operations/threat-finance-and-financial-intelligence/

agencies and industry sectors. ACAMS circulates and discusses the latest trends and case studies in money laundering and terrorist financing through seminars, forums, international conferences, and local chapters.[20] The participation of senior U.S. government officials from the Departments of Treasury, Justice, and Homeland Security, the bank regulators, and law enforcement agencies, responsible for combating terrorist financing and money laundering, at ACAMS events demonstrates the active outreach conducted by the U.S. government to promote public-private partnerships.

Countering Emerging Threats to the Financial Sector

Another example of cross-sector collaboration to protect the international financial system is the Financial Services Information Sharing and Analysis Center (FS-ISAC.) It serves as the global financial industry's "go-to" resource for cyber and physical threat intelligence analysis and sharing. FS-ISAC is unique in that it was created by and for members in 1999 to prepare for Y2K and operates as a member-owned nonprofit entity. It was established by the financial services sector in response to the 1998 Presidential Directive 63, (later updated by the 2003 Homeland Security Presidential Directive 7) that mandated that the public and private sectors share information about physical and cyber security threats and vulnerabilities to help protect the U.S. critical infrastructure, of which the financial sector is a vital component.[21]

In response to emerging global threats in cyberspace to the financial sector, FS-ISAC's board extended its charter in 2013 to share information among financial services firms around the world. Constantly gathering reliable and timely information from financial services providers, commercial security firms, federal/national, state and local government agencies, law enforcement and other trusted resources, the FS-ISAC can quickly disseminate physical and cyber threat alerts and other critical information to other organizations. This information includes analysis and recommended solutions from leading industry experts.

[20] ACAMS Mission website, http://www.acams.org/join-acams/#tabbed-nav=what-is-acams
[21] Financial Services Information Sharing and Analysis Center website, https://www.fsisac.com/about

The Center's Critical Infrastructure Notification System (CINS) allows the FS-ISAC to send security alerts to multiple recipients around the globe near-simultaneously, while providing for user authentication and delivery confirmation. The system also provides an anonymous information sharing capability across the entire financial services industry; this protects members' proprietary information and client confidentiality. When they receive a submission, industry experts verify and analyze the threat and identify any recommended solutions before alerting FS-ISAC members. This procedure assures that member firms receive the latest tried-and-true procedures and best practices for guarding against known and emerging security threats.[22] Peer-to-peer collaboration brokered by formal organizations like FS-ISAC, combined with notifications to the appropriate government officials in the U.S. and elsewhere, is an example of timely and effective mechanisms to detect, address, and prevent threats to the financial system in the traditional and cyber domains.

International Cooperation and Public-Private Partnerships

Unilateral, individual country efforts are not enough to counter terrorist financing and money laundering. Our international financial system is far more interconnected and interdependent than ever before. International cooperation between the public and private sectors is therefore paramount. The Financial Action Task Force (FATF) is an inter-governmental body established in 1989 by the ministers of its 34 member jurisdictions. The FATF sets standards and promotes effective implementation of legal, regulatory and operational measures for combating money laundering, terrorist financing and other related threats to the integrity of the international financial system. It serves as a "policy-making body" working to generate the necessary political will to bring about national legislative and regulatory reforms to protect in the global financial system. The FATF has developed a series of recommendations that are recognized as the international standard

[22] *Ibid.*

for combating of money laundering and the financing of terrorism and proliferation of weapons of mass destruction.[23]

The FATF values private sector expertise and operational knowledge, as essential resources to evaluate the application of the AML/CFT requirements to business practices, and to encourage the practical adoption of the standards. The private sector can serve as a helpful sounding board to "test" or assess the potential impact of measures under consideration, or brainstorm on possible technical solutions in a specific field affecting the financial industry. It is also an important way to learn about market developments and access new information regarding emerging threats and vulnerabilities to the global financial system.[24] The FATF Private Sector Consultative Forum is the formal means to reach out to and cooperate with private sector stakeholders. It holds open consultations with interested stakeholders and sets up working groups to examine specific issues including financial innovations like mobile payments, virtual currencies, store of value cards that could be vulnerable to money laundering or terrorist financing.[25] These examples of domestic and international public-private partnership have strengthened the international financial system to detect and deter terrorist financing, money laundering and other financial crimes. According to declassified intelligence reports, groups like Al Qaeda and the Mexican drug cartels decided to refrain from using the formal banking sector due to the enhanced compliance and monitoring measures adopted by the private sector.

Strengthening U.S. Capabilities and Promoting Public-Private Sector Collaboration to Combat Terrorism, Crime and Corruption

The U.S. and its allies have increased their efforts to detect the financing of terrorism and crime, levied economic sanctions, and raised awareness among the private

[23] FATF website, http://www.fatf-gafi.org/about/
[24] FATF Recommendations 2012, "Public and private sector partnership in fighting financial crime," http://www.fatf-gafi.org/documents/documents/publicandprivatesectorpartnershipinfightingfinancialcrime.html
[25] FATF "G8 Public-Private Sector Dialogue on anti-money laundering and countering the financing of terrorism (AML/CFT)," http://www.fatf-gafi.org/publications/fatfgeneral/documents/ppsdsept13.html

and civic sectors about how bad actors can exploit the international financial system to fund their networks and deadly operations. These endeavors to leverage the financial instrument of national power against terrorism, crime and corruption are laudable but could be further expanded at the national, regional and international levels with the following measures:

1. Integrate the financial instrument of national power more deliberately into future U.S. strategies to counter emerging transnational threats;
2. Strengthen U.S. and international financial intelligence and information-sharing mechanisms to more effectively combat terrorism, crime and corruption;
3. Dedicate more financial, human and technological resources to government agencies, responsible for investigating, prosecuting and countering terrorist financing, money laundering and other financial crimes. The 2017 fiscal year budget request for the Treasury Department for the Office of Terrorism and Financial Intelligence was only $117 million to curb terrorist financing, including ISIL financing, and to implement sanctions targeting Iran, North Korea, Syria, as well as $115 million for the Financial Crimes Enforcement Network.[26]
4. Set aside a percentage of forfeited assets and/or fines levied on financial institutions for sanctions evasion, money laundering and compliance infractions to fund domestic and international capacity building programs;
5. Retain and expand a vigorous designation and sanctions regime against state sponsors of terrorism, foreign terrorist organizations, transnational criminal organizations, foreign narcotics kingpins and specially designated nationals;
6. Promote public-private partnerships; raise awareness among bank and non-bank financial institutions of emerging trends in money laundering and terrorist financing to keep up with the unprecedented pace of technological change;
7. Empower the private and civic sectors to actively to detect and deter financial crimes and contribute to counter threat finance strategies and operations; and

[26] U.S. Department of Treasury FY2017 Budget in Brief Fact Sheet, https://www.treasury.gov/about/budget-performance/budget-in-brief/Documents/FY17FactSheet.pdf

8. Encourage more formal research and study of the illicit economy and anticipate how new financial innovations, services, technology, such as virtual currencies and block chain, could possibly be used and abused by terrorists and criminals to finance and facilitate their operations.

In conclusion, terrorists, criminals and their facilitators are presenting complex, asymmetrical threats to U.S. national security interests at home and abroad. The dangerous convergence of illicit networks challenges the sovereignty, security and prosperity of the nation state and must be actively addressed. These illicit networks require critical enablers, most importantly financing, to realize their destructive agendas of terrorism or crime. Stemming the flow of funding to groups, like ISIL, can significantly degrade their violent operations and impact. As these illicit networks adapt and evolve, we must constantly update our methods of detecting, disrupting, dismantling and deterring our adversaries with the financial instrument of national power. Only through proactive interagency, multi-sectorial and international strategies can we effectively counter terrorism, crime and corruption around the world.

Thank you, Mr. Chairman and committee members for your time and attention.