COUNTERING THE FINANCIAL NETWORKS OF WEAPONS PROLIFERATION

HEARING

BEFORE THE

SUBCOMMITTEE ON TERRORISM AND ILLICIT FINANCE

OF THE

COMMITTEE ON FINANCIAL SERVICES

U.S. HOUSE OF REPRESENTATIVES

ONE HUNDRED FIFTEENTH CONGRESS

SECOND SESSION

JULY 12, 2018

Printed for the use of the Committee on Financial Services

Serial No. 115–108

U.S. GOVERNMENT PUBLISHING OFFICE

31–507 PDF WASHINGTON : 2018

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
STEVAN PEARCE, New Mexico
BILL POSEY, Florida
BLAINE LUETKEMEYER, Missouri
BILL HUIZENGA, Michigan
SEAN P. DUFFY, Wisconsin
STEVE STIVERS, Ohio
RANDY HULTGREN, Illinois
DENNIS A. ROSS, Florida
ROBERT PITTENGER, North Carolina
ANN WAGNER, Missouri
ANDY BARR, Kentucky
KEITH J. ROTHFUS, Pennsylvania
LUKE MESSER, Indiana
SCOTT TIPTON, Colorado
ROGER WILLIAMS, Texas
BRUCE POLIQUIN, Maine
MIA LOVE, Utah
FRENCH HILL, Arkansas
TOM EMMER, Minnesota
LEE M. ZELDIN, New York
DAVID A. TROTT, Michigan
BARRY LOUDERMILK, Georgia
ALEXANDER X. MOONEY, West Virginia
THOMAS MACARTHUR, New Jersey
WARREN DAVIDSON, Ohio
TED BUDD, North Carolina
DAVID KUSTOFF, Tennessee
CLAUDIA TENNEY, New York
TREY HOLLINGSWORTH, Indiana

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
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
BILL FOSTER, Illinois
DANIEL T. KILDEE, Michigan
JOHN K. DELANEY, Maryland
KYRSTEN SINEMA, Arizona
JOYCE BEATTY, Ohio
DENNY HECK, Washington
JUAN VARGAS, California
JOSH GOTTHEIMER, New Jersey
VICENTE GONZALEZ, Texas
CHARLIE CRIST, Florida
RUBEN KIHUEN, Nevada

SHANNON MCGAHN, *Staff Director*

SUBCOMMITTEE ON TERRORISM AND ILLICIT FINANCE

STEVAN PEARCE, New Mexico *Chairman*

ROBERT PITTENGER, North Carolina, *Vice Chairman*
KEITH J. ROTHFUS, Pennsylvania
LUKE MESSER, Indiana
SCOTT TIPTON, Colorado
ROGER WILLIAMS, Texas
BRUCE POLIQUIN, Maine
MIA LOVE, Utah
FRENCH HILL, Arkansas
TOM EMMER, Minnesota
LEE M. ZELDIN, New York
WARREN DAVIDSON, Ohio
TED BUDD, North Carolina
DAVID KUSTOFF, Tennessee

ED PERLMUTTER, Colorado, *Ranking Member*
CAROLYN B. MALONEY, New York
JAMES A. HIMES, Connecticut
BILL FOSTER, Illinois
DANIEL T. KILDEE, Michigan
JOHN K. DELANEY, Maryland
KYRSTEN SINEMA, Arizona
JUAN VARGAS, California
JOSH GOTTHEIMER, New Jersey
RUBEN KIHUEN, Nevada
STEPHEN F. LYNCH, Massachusetts

CONTENTS

WITNESSES

THURSDAY, JULY 12, 2018

APPENDIX

ADDITIONAL MATERIAL SUBMITTED FOR THE RECORD

COUNTERING THE FINANCIAL NETWORKS OF WEAPONS PROLIFERATION

Thursday, July 12, 2018

U.S. HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON TERRORISM
AND ILLICIT FINANCE,
COMMITTEE ON FINANCIAL SERVICES,
Washington, D.C.

The subcommittee met, pursuant to notice, at 2:04 p.m., in room 2128, Rayburn House Office Building, Hon. Stevan Pearce [chairman of the subcommittee] presiding.

Present: Representatives Pearce, Pittenger, Rothfus, Tipton, Williams, Poliquin, Emmer, Zeldin, Davidson, Budd, Maloney, Himes, Foster, Sinema, Gottheimer, and Lynch.

Chairman PEARCE. The subcommittee will come to order. Without objection, the Chair is authorized to declare a recess of the subcommittee at any time. Members of the full committee who are not members of the Subcommittee on Terrorism and Illicit Finance may participate in today's hearing and all members will have five legislative days within which to submit extraneous materials to the Chair for inclusion in the record.

This hearing is entitled, "Countering the Financial Networks of Weapons Proliferation." I now recognize myself for 2 minutes to give an opening statement. First of all, I want to thank everyone for joining us today. Today's hearing will examine the financial networks that support nuclear, chemical, and biological weapon productions, the role of the U.S. in counter-proliferation finance efforts, and the scope and effectiveness of the relevant enforcement actions by the U.S. to counter-proliferation financing.

Hostile nations often use established financial mechanisms such as wire transfer, trade finance products, cash, checks, and credit cards to finance their weapons programs. This is accomplished through elaborate ownership structures consisting of various businesses, shell corporations, and middlemen that are often used to obscure any connection to the country proliferating weapons.

As these bad actors continue to evolve in the ways that they access the traditional financial marketplace, we must ensure that our Government agencies and financial institutions have the tools necessary to detect illicit procurement efforts. Evidence has shown that hostile actors around the world have pursued the proliferation of various weapons for years, as country sanctions and even secondary sanctions are implemented, removed, or modified, a balance must be struck.

Financial institutions should work together to prevent illicit financing while providing agreed upon market access. In today's hearing, I hope to discuss what methods are being used to circumvent sanctions to finance weapons proliferation, what tools and partnerships are working well to detect and disrupt procurement networks, and what challenges remain for Government authorities and financial institutions to identify proliferation activities.

I would also appreciate any comments about deficiencies and weaknesses in the international system and how the United States can best assist to ensure that the funding of proliferation can effectively be stopped in this dynamic environment. I am especially interested in hearing about this in light of the United States assuming the presidency of the Financial Action Task Force this month.

I would like to thank our witnesses for being here today and I look forward to their expert testimony on these very important issues.

The Chair now recognizes Mr. Foster for 5 minutes for an opening statement.

Mr. FOSTER. Thank you, Mr. Chairman. And I would like to thank all of our distinguished witnesses for testifying this afternoon. Today, the subcommittee is going to examine strategies to disrupt the financing and procurement of weapons of mass destruction. We are at an interesting time in our history to say the least.

We have a number of potential threats. These include not very well-organized groups trying to get the parts together for a dirty bomb. We have states, for example, Iran, who are looking to assemble a bomb factory. And we are talking also about stolen nuclear weapons from states where the security is not so great.

And finally, the big issue of making sure that we have complete and verifiable denuclearization of North Korea, a much more difficult problem where we are looking not for a bomb factory but for a single completed bomb secreted away anywhere in that country. And so in all but the last case, there are significant signatures to go after and some of the most significant ones are the financial footprints that lead to that. And that is why this hearing is important.

For nearly a generation, nuclear weapons have threatened our national security and global safety because of their capability to threaten the existence of mankind. And unfortunately, this ability is no longer unique to just nuclear weapons. The proliferation of emerging technologies, chemical, biological, and radiological weapons, and the related delivery system pose a real risk to our international security.

Even today, rogue regimes and clandestine organizations continue to exhibit the ambition to acquire materials and technologies that can be used to build weapons of mass destruction, which is why despite many challenges, prevention of the distribution and financing of these weapons remains a major U.S. policy objective.

To date, the international community has utilized a variety of tools to accomplish this including export controls, sanctions, anti-money laundering (AML) laws, and international treaties. But despite these measures, proliferators have continued to use the financial system with relative ease to facilitate their illicit procurement of materials.

Alternative and creative sources of funding have allowed them the ability to circumvent the global counter-proliferation financing rules and many of the standard detection methods, posing a major obstacle for law enforcement and the intelligence community.

On July 1, 2018, the United States assumed the position of the president of the Financial Action Task Force (FATF), an inter-governmental body tasked with developing and promoting policies to combat money laundering and terrorist financing. This presents an invaluable opportunity for us to highlight the criticality of this issue within the organization's already established framework and to show leadership in important multilateral collaborations.

Going forward, we must encourage the use of technological innovations and policies that improve our counter-proliferation efforts. I look forward to hearing your testimony and yield back the balance of my time.

Chairman PEARCE. The gentleman yields back. The Chair now recognizes the gentleman from North Carolina for 3 minutes for an opening statement.

Mr. PITTENGER. Thank you, Mr. Pearce and Congressman Foster, for holding this hearing today. Additionally, I would like to thank all of our witnesses for coming in today to provide us with their expertise in our efforts to counter the financing of weapons proliferation.

As technology progresses, terrorist networks acquire new means for acquiring the illicit financing needed to procure weapons of mass destruction. The most important step in protecting our national security, and that of our allies, is to prevent these organizations from acquiring these weapons.

Traditional financial mechanisms such as cash, credit cards, or wire transfers are often used by proliferation networks to facilitate their funding activities. We already know these mechanisms and must continue to ensure we are capable of identifying their use for malicious purposes and preventing them.

However, we must focus our efforts on ensuring we are able to combat the use of new mechanisms that have developed with today's technology for the purposes of financing weapons proliferation. Such mechanisms include the use of blockchain technology which serves as the public transaction ledger for bitcoin, other forms of cryptocurrency, or online crowd funding websites.

While these financial mechanisms provide various positive and valuable opportunities, they are also very popular with terrorist networks due to the anonymity that is associated with their utilization. There is a global black market for nuclear technology and material that we must work to detect and eradicate.

Hostile state actors which have been involved with this market pose a serious threat to our national security. States such as Iran can also use front companies to acquire critical nuclear technologies with use of intermediate jurisdictions in order to obfuscate our efforts in tracing their transactions.

Learning how to better combat such practices in order to ensure sanctions are not evaded must be a priority. Additionally, we must strategize how to assist other nations with their capabilities to prevent proliferation financing. There are numerous countries which are currently not able to successfully prevent proliferation financ-

ing, and this poses an obstacle to global counter-proliferation efforts.

We look forward to learning how we can expand our efforts in combating illicit finance for weapons proliferation. Thank you, Mr. Chairman. I yield back the balance of my time.

Chairman PEARCE. Gentleman yields back. Today, we welcome the testimony of our witnesses. Mr. David Albright is a physicist, is founder and President of the non-profit Institute for Science and International Security in Washington, DC. Notably, the institute publishes the Peddling Peril Index that ranks countries according to their capabilities and demonstrated success in implementing strategic export controls to prevent nuclear trafficking.

Mr. Albright has been called the go-to guy for media seeking independent analysis of Iraq's weapons program. In June 1996, he was the first non-governmental inspector of the Iraqi nuclear program. Prior to founding the Institute for Science and International Security in 1993, Mr. Albright was a senior staff scientist at the Federation of American Scientists and a member of the research staff of Princeton University's Center for Energy and Environmental Studies.

Mr. Albright received Masters of Science in physics from Indiana University in 1980, Masters of Science in mathematics from Wright State University in 1977, and a Bachelor of Science from Wright State University, 1975.

Mr. Tom Keatinge is Director of the Center for Financial Crime and Security Studies at the Royal United Services Institute for Defense and Securities Studies, better known as RUSI. RUSI is headquartered in London and is the oldest defense and security think tank in world. Mr. Keatinge primarily researches areas including terror finance, counter-proliferation finance, new approaches to tackling financial crimes in human trafficking, as well as corruption and the implementation of financial sanctions. Prior to joining RUSI in 2014, he was an investment banker at JPMorgan for 20 years.

Mr. Keatinge has a Masters in intelligence and international security from Kings College London. This is Mr. Keatinge's first Congressional testimony in the United States. Thank you for traveling all this way to speak to us. And stop by New Mexico and spend money out there, too, on the way home.

Mr. Ottolenghi is a Senior Fellow at the Foundation for Defense of Democracies or FDD, an expert at its Center on Sanctions and Illicit Finance. At FDD, he focuses on Iran's history of sanctions evasion. His researches examine Iran's Islamic Revolutionary Guard Corps including its links to the country's energy sector and procurement networks.

Prior to joining FDD, Dr. Ottolenghi headed the Trans-Atlantic Institute in Brussels and taught Israel studies at St. Anthony's College, Oxford University. He obtained his PhD in Political Theory at the Hebrew University of Jerusalem preceded by undergraduate studies in political science at the University of Bologna.

Ms. Elizabeth Rosenberg is a Senior Fellow and Director of Energy and Economics and Security Program at the Center for New American Security, CNAS. In this capacity, she publishes and speaks on the national security and foreign policy implications of

energy market shifts and the use of sanctions and economic statecraft.

She has testified before Congress on energy and financial issues and we welcome her back. From May 2009 through 2013, Ms. Rosenberg served as a senior advisor to the assistant secretary for terrorist financing and financial crimes and then to the undersecretary for terrorism and financial intelligence at Treasury. She received an MA in Near Eastern Studies from New York University and a BA in politics and religion from Oberlin College.

Each of you are going to be recognized for 5 minutes to give an oral presentation of your testimony. Without objection, each of your written statements will be made part of the record. Mr. Albright, you are recognized for 5 minutes.

STATEMENT OF DAVID ALBRIGHT

Mr. ALBRIGHT. Thank you, Chairman Pearce and Ranking Member Foster, for the opportunity to testify today. As the chairman mentioned, my institute recently published a report ranking the export control systems of 200 countries and territories based on their capabilities and performance in five areas addressing export control legislation, international commitments, illicit procurement detection, enforcement, and financing of proliferation.

Preventing proliferation financing, albeit not a traditional component of a review of national export control systems, is one of the most important aspects for detecting and stopping exports of sensitive goods. To measure a country's ability to prevent proliferation financing, we used a set of criteria that indicate a country's susceptibility to being exploited or involved in proliferation financing including violations of international sanctions.

These criteria are based on countries' financial regulatory systems and counter illicit financing programs from which the main source of data for the index is a Financial Action Task Force, FATF. Our research for the 2017 ranking revealed that preventing proliferation financing is one of the counter-proliferation areas most in need of improvement. This effort would benefit significantly from a closer integration with export controls.

In the ranking of a country's ability to prevent proliferation financing, no country achieved two-thirds of the available points and only two received more than half the available points. About one-third of all countries achieved negative scores. Among others, significant illicit financial flows, big black markets, and high levels of corruption indicate that those countries are likely places where front companies find it relatively easy to finance nefarious activities.

Other countries performed poorly due to having excessive bank secrecy, providing tax havens, or simply lacking regulations and effective institutions. A preliminary update for 2018 on preventing proliferation financing show similar results. Countries still performed poorly and only three countries received 50 percent and more of the possible points.

Iran performs particularly poorly in the index including on proliferation financing where it ranked on the bottom. Iran has been given extended time to fulfill its action plan requirements set out by the FATF and to comply with FATF standards. Recent actions

have confirmed a deep involvement of Iran's financial system in illicit activities. As a result, we recommend the re-imposition of FATF counter-proliferation measures against Iran.

The institute has developed a range of other recommendations while producing the Peddling Peril Index and working with proliferation financing experts to develop the index's methodology.

One of the most critical recommendations is that countering proliferation financing needs to be integrated into other aspects of counter-proliferation including export controls. And I would like to highlight five other recommendations.

All countries should work closely with FATF and its regional bodies to improve their efforts to prevent proliferation financing. Each country should conduct a risk assessment of proliferation financing and its agencies should address any gaps identified.

Each government should have adequate legislation in place that includes an effective system of coordination among the departments working on proliferation financing, such as well-resourced investigative financial intelligence units and effective outreach to financial institutions.

Countries' financial institutions need to be able to monitor, detect, report, and act upon suspicious financial transactions. Countries should help financial institutions identify and freeze suspicious transactions.

Because of the difficulty of accomplishing this goal, the U.S. Government should launch an inter-agency study to improve communication and information sharing with financial institutions, including insurance companies, and to develop better solutions for automated counter-proliferation financing screening tools.

FATF is in a unique position to drive many of the abovementioned recommended actions and changes and should do so. Financing of proliferation should be treated broadly and as a separate subject to money laundering and terrorist financing.

At the plenary meetings, the FATF working group should discuss adjusting the language in several of the existing 40 FATF recommendations to extend them beyond terrorist financing and money laundering to include proliferation financing. Thank you for the opportunity to testify. I am happy to answer any questions.

[The prepared statement of Mr. Albright can be found on page 42 of the appendix.]

Chairman PEARCE. Thank you, sir.

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

STATEMENT OF TOM KEATINGE

Mr. KEATINGE. Chairman Pearce, Ranking Member Foster, and distinguished members of the subcommittee, thank you for inviting me to testify today, my first opportunity to do so. Given my home base in London and the focus of RUSI's counter-proliferation finance research is on Southeast Asia and Sub-Saharan Africa, my testimony and contribution will necessarily address, to a greater extent, the international CPF architecture as promoted by bodies such as the U.N. and the Financial Action Task Force rather than the policies laid out the U.S. domestic agencies.

However, as has been mentioned with the U.S. taking over presidency of the Financial Action Task Force the next 12 months, the

U.S. has a key role to play in strengthening this weak architecture. You will be familiar with the CPF requirements set forth by the FATF standards and the evaluations undertaken by the FATF. The U.S. evaluation was published in December 2016.

As indicated by the table provided in my written submission, the international CPF effort is disappointing. Two-thirds of assessed countries are non or only partially compliant with the requirements to be able to impose targeted financial sanctions without delay. And 70 percent of assessed countries have a low or moderate level of effectiveness, meaning they suffer from major shortcomings.

It is clear that notwithstanding the prioritization of CPF in 2012 by the FATF, the global community still has considerable work to do to harden the financial system against abuse by proliferators. And it is important to note that compliance with FATF standards alone does not result in effective CPF controls.

In fact, FATF's recommendations are now increasingly out of touch with other international obligations on CPF. U.N. sanctions against North Korea incorporate measures that go beyond list-based sanctions implementation and focus, to a greater extent, on activity-based obligations to counter-proliferation finance.

How do we secure the financial system against abuse by proliferators? Proliferation activities are made possible by the international financial system. Reports from the U.N. panel of experts highlight that Pyongyang is using greater ingenuity in accessing formal banking channels to support illicit activities in WMD (weapons of mass destruction) proliferation and continues to access the international financial system because of critical sanctions implementation deficiencies.

The role played by the financial sector in disrupting proliferation finance has received greater attention in recent years. Some governments maintain that financial institutions have both the capability to detect and an obligation to disrupt financial transactions in support of illicit WMD proliferation.

However, government initiatives on counter-proliferation finance vary widely between jurisdictions and often in our experience are nonexistent. Our research reveals extensive gaps in knowledge, awareness, and capabilities of banks and perhaps more worryingly, highlights considerable misunderstanding with regards to the risks posed by proliferators, often conflating CPF activity with sanctions compliance.

It is therefore important that financial institutions take time to better understand and mitigate proliferation financing risk. But it's not just in banking where vulnerability exists. As actual sanctions have been increasingly applied to North Korea, it is undertaking creative, deceptive activity to secure funding from the sale of coal and it is also undertaking at sea ship-to-ship transfers to secure the energy products it needs.

These activities bring into scope other industries needed to secure the integrity of the international supply chain that would benefit from engagement with national governments such as shipping companies, commodity brokers, and insurance companies, all of which lag the banking sector in terms of awareness of and capability and commitment to the global CPF agenda. Whilst the banking sector must continually strive to improve its standards, a whole

system approach is need in order to maximize disruption opportunities.

To conclude, as evidence by the FATF's evaluation data and the detailed reports that the U.N. panel of experts on North Korea, 6 years since the FATF introduced CPF as a third leg of focus alongside money laundering and terrorist financing, global CPF efforts are fragmented at best and ineffective and non-existent at worst.

Furthermore, the current FATF standards related to CPF are weak and simplistic. They do not require countries to assess their proliferation financing risks, they focus merely on the implementation of targeted financial sanctions and they are not risk-based in their application.

In sum, the global architecture for disrupting proliferation finance requires improved design and implementation. In my submission, I have set forth recommendations to the private sector, international organizations such as the FATF, the U.S. Government and international governments that I hope we can discuss further during the session. Thank you once again for the opportunity to testify today.

[The prepared statement of Mr. Keatinge can be found on page 65 of the appendix.]

Chairman PEARCE. Thank you, sir. Mr. Ottolenghi, 5 minutes.

STATEMENT OF EMANUELE OTTOLENGHI

Mr. OTTOLENGHI. Chairman Pearce, Ranking Member Foster, and distinguished members of the subcommittee, I want to thank you for the opportunity to have me here to testify. The Islamic Republic of Iran has been under U.S. sanctions since late 1979. From 2006 to 2016, Iran's nuclear and ballistic missile programs were the target of a United Nations sanction regime which the United States, the European Union, and their western allies subsequently expanded with their own set of far-reaching measures.

Initially designed to punish and prevent proliferation attempts, sanctions eventually became wider in scope, targeting Iran's energy industry, financial sector including its Central Bank, shipping, aviation, insurance, and oil exports.

Beginning in January 2016, the Joint Comprehensive Plan of Action or JCPOA granted Iran's sanction relief though not to non-nuclear sanctions. Due to the president's May 2018 decision to withdraw from the JCPOA, Iran again faces U.S. sanctions including secondary sanctions, which are already causing numerous international companies to withdraw from the Iranian market.

Iran is therefore likely to ramp up its sanction evasion efforts. Sanctions significantly inhibit Tehran's ability to trade with the world, still, Iran has adapted, engaging sanctions enforcers in a complex and evolving cat and mouse game. To put it bluntly, for Iran, sanctions are temporary roadblocks, not insurmountable obstacles.

By building bypass roads, Iran turns crisis into opportunities. As a result, Iran has been able to mitigate sanctions impact on its efforts to advance its nuclear and ballistic missile programs. My written testimony illustrates how Iran evaded sanctions in the past offering typologies as well as case studies.

Let me briefly outline some of these practices. Procurement usually relies on a triangular structure of front companies operating overseas, Iranian proxies establish fronts in a foreign country to procure dual use technologies. Once incorporated, companies buy locally or from a third country. The buyer then ships the procured goods to a final destination in Iran or fictitiously sells them to another front company in another country before final delivery.

These cases typically involve small companies which will shut down once they have accomplished their mission. For longer term procurement and finance operations, Iran relies more on permanent and more complex corporate structures across different jurisdictions. Their link with an Iranian parent entity is purposely made less obvious.

Iranian senior corporate managers often fictitiously resign their government jobs to seek business ventures overseas on behalf of the regime, quickly emerging as proprietors of business empires with no formal ties with Iran. A regime proxy with no formal connection to past employers provides plausible deniability.

Former regime procurement agents interviewed by FDD confirmed that Iranian state companies have increasingly entrusted their most capable senior management with significant sums to invest in industrial assets abroad.

This includes ownership of western factories which gives Iran access to knowledge and technology. This was the case in 2013 of MCS International in Germany. Regime agents bought the factory to lay their hands on a dual use flow forming machine that MCS production line used to shape gas cylinders. Such machines are also critical in the production of uranium enrichment centrifuges.

Iran's evasion of financial sanctions follows the same playbook. The regime first established and then sought to purchase banks outside Iran to facilitate prohibited banking transactions adding successive layers of obfuscation to cover its tracks.

This was the case for example with InvestBank in the Republic of Georgia. The network associated with the bank used shell companies in Canada, the U.S., Georgia, Lichtenstein, Switzerland, Turkey, New Zealand, and the UAE to launder billions of dollars according to U.S. court documents while also procuring and shipping technology to Tehran, likely on an airline owned by the network.

Regime has also been very capable of exploiting loopholes in sanctions legislation. One such case was the gas for gold scheme its proxies ran through Turkey and which I describe at length in my written statement.

The regime will not hesitate to invest significant resources to facilitate these activities and empower its agents. A typical ancillary service its agents rely upon is the acquisition of passports of convenience usually through costly citizenship by investment schemes to be able to travel, incorporate companies, and open bank accounts hassle-free.

Iranian sanction evasion activity follows established patterns, financial institutions and intelligence practitioners can study these typologies to identify actors in transactions that are potentially harmful to the integrity of the financial system or pose challenges to international security. Treasury plays a key role in this regard,

its designations have helped expose Iranian efforts to circumvent sanctions.

But as indicated before, this is a cat-and-mouse game, where one can never assume that countermeasures are the final word as Iran will seek a way around them. This is just one of the topics in my recommendations which I offered in my written statement.

I do thank you for your time and the invitation once again. And I look forward to your questions. Thank you.

[The prepared statement of Mr. Ottolenghi can be found on page 75 of the appendix.]

Chairman PEARCE. Thank you, sir.

Ms. Rosenberg, for 5 minutes.

STATEMENT OF ELIZABETH ROSENBERG

Ms. ROSENBERG. Thank you, Chairman Pearce, Ranking Member Foster, and distinguished members of this committee for the opportunity to speak today on countering the financial networks of weapons proliferation.

The financing of weapons of mass destruction proliferation is a grave threat facing the United States and the global financial system. The ability of rogue states or non-state actors to obtain weapons of mass destruction by using illicit financial activity and procurement networks is a major challenge to the U.S., to U.S. foreign policy goals, to the security of our homeland and that of our partners, and to the integrity of the global financial system and the global nonproliferation regime.

Countering proliferation finance must be a core part of the policy approach to the United States' most pressing national security concerns, specifically North Korea, Iran, and Syria. Furthermore, the United States must lead on this issue in international forums, doing much more than the present nascent measures.

This essential work is undeniably challenging. Proliferation finance is difficult to detect. It is hidden within shell companies and among legitimate financial transactions. Looking for it is a technically challenging exercise at the intersection of sanctions enforcement, export controls, financial crimes compliance, and the global nuclear nonproliferation regime.

As counter-proliferation finance work must operate across multiple jurisdictions, involve an array of different constituencies with different legal and regulatory authorities which have various privacy and data sharing obligations, and with major differentiation in political will and technical capacity, coordinating a truly effective international response is not easy.

But the difficulties associated with countering the financing of proliferation should not give the false impression that creating a more effective policy framework is beyond the capacity of the international community.

We know the deficiencies in the system. We certainly care about nuclear security and we can do better. Let us start with the regulatory regime. Compliance and oversight programs for financial institutions have historically focused on financial integrity threats other than proliferation finance, like anti-money laundering and anti-corruption, and countering terrorist financing efforts.

Proliferation, including by North Korea and Iran, is no less significant as a security threat and must be treated as such. If policy leaders clarify that proliferation finance is on par with the obligation to counter terrorism, for example, it will go a long way to raise the profile of this issue and improve controls around it.

This can have a direct benefit in improving the ability of vulnerable jurisdictions such as Hong Kong or Malaysia, for example, to deny proliferators safe haven and safe passage for their money. The United States should be the gold standard for information sharing relevant to proliferation finance between institutions, with governments, and across jurisdictions.

Sections 314(a) and (b) of the USA PATRIOT Act are good models for creating the operational ability to facilitate information sharing, but policymakers must focus on expanding and incentivizing the use of these measures and in urging adoption of parallel measures in other jurisdictions.

U.S. policy leaders must also work with international counterparts to harmonize such data sharing measures with privacy regulations so that justifiable concerns about misuse of personal data do not prevent cooperation and disrupting and preventing proliferation, an important law enforcement and international security priority.

Congress has a direct role to play and encouraging more information collection, analysis, and public disclosure around proliferation finance. This includes supporting rigorous customer due diligence (CDD) practices by banks, by not allowing anonymous companies to abuse our financial system, and by supporting a regulatory sandbox and safe harbor provisions to incentivize creative strategies to counter proliferation finance.

And Congress must aggressively encourage the Administration to publicly and privately disclose proliferation finance data and typologies including via FinCEN (Financial Crimes Enforcement Network) advisories. Moreover, Congress should strongly support the Administration in its new role as the Financial Action Task Force president, as has been discussed by several of my co-panelists here, to set tough new international guidelines for tracking and sharing information on proliferation finance, and for taking that action at the national level.

I want to close by stating how grave the consequences are for failing to appreciate the seriousness of the proliferation finance threat. Complacency and policy inaction are weak links that help U.S. adversaries to actively and alarmingly develop nuclear weapons capabilities; the stakes could not be higher.

Thank you for your attention and I look forward to answering questions you may have.

[The prepared statement of Ms. Rosenberg can be found on page 92 of the appendix.]

Chairman PEARCE. Thanks each one of you for your presentations. I yield myself now 5 minutes for questions. First, so just looking at the complexity of tracking the financial aspects and the shell corporations, just everything is very complex.

The sanctions have, it sounds like according to your testimony, an effect, but also it is very difficult for financial institutions to assess who the players are that are legitimate, who are not, legiti-

mate transactions versus those that are gearing toward proliferation.

I guess my question is how do we get around this obscurity? Let us back that up one section and say when a major—can we assess that most of the compromises of our sanctions are purposeful or just plain inability to see?

Mr. Keatinge, do you want to take a shot at that? I know it is just going to be a guess but—

Mr. KEATINGE. We are sitting here in the United States, surrounded by a sophisticated financial system. And yes, we are right that front companies and all of these are used to try and obfuscate the movement of funds.

But let us not forget, look in the U.N. panel report and it is a litany of failures in countries where it is just that they don't understand the risk that they are faced with.

Chairman PEARCE. And what would we do to drive the understanding?

Mr. KEATINGE. Your government spends a lot of money providing technical assistance and awareness raising to countries like Uganda, Tanzania, Mozambique, these kinds of countries where North Korea are earning money, raising money through providing services that they can then spend on their proliferation ambition.

I think it is a polarized position here. There is raising very basic standards, implementing basic understanding, which is what we would expect the FATF to be doing. And then there is dealing with the more complex structures and obfuscation that the other panelists have spoken about.

And yes, there are financial institutions that will no doubt facilitate the illicit movement of finance knowingly. Equally, there are many financial institutions that do that without realizing they are doing it because of the complexity of the structures that they use.

Chairman PEARCE. OK. Mr. Ottolenghi, on page two you talk about the adapting of the purchasing system. I assume that means that we start with a legitimate purchasing system and then we begin to adapt and we get people who are selling to the companies familiar and then they adapt it closer and closer to proliferation. Is that correct?

Mr. OTTOLENGHI. Absolutely correct, yes.

Chairman PEARCE. OK. Then is it a profit motive? Is it just your complacency? Is it a combination of corruption and a profit motive and complacency that would drive the companies to continue selling? They just don't watch that close? Tell me a little bit about that.

Mr. OTTOLENGHI. It is a combination. On the part of those involved in helping, assisting Iran to procure, there is the profit. Sometimes there is also the ideology but more often than not the two things converge.

Chairman PEARCE. It gets pretty difficult to assess precisely. Ms. Rosenberg then, so listening to that particular thing, do you think there would be advantage to having some piece of the sanctions push downstream to people who, either through carelessness or whatever, they began to feel, not the full sanctions but, sanctions of some sort against them.

If they just didn't pay attention, they are corrupt, we can assess their mindset. Is it possible to have the sanctions move downstream to the places where the financing is coming from? Is that too difficult?

Ms. ROSENBERG. There are many opportunities to use sanctions to advance our counter-proliferation objectives. A primary focus area that we should attend to now is the lack of political will to enforce obligations. Just because the U.N. has sanctions, just because the United States has sanctions, does not mean that people are following them.

Chairman PEARCE. OK, let me catch you right here though, that the U.S. has invoked sanctions on countries where we are trying to stop the proliferation and the countries where the will is lacked, our sanctions to North Korea or Iran or whoever would begin to percolate downstream to those that don't have a strong motive for interrupting. Is that too egregious?

Ms. ROSENBERG. There are opportunities.

Chairman PEARCE. Take a quick shot. I want Mr. Ottolenghi to address it too.

Mr. OTTOLENGHI. I just want to give an example.

Chairman PEARCE. Yes, let her finish. And then I will come to you, just 19 seconds, so—

Mr. OTTOLENGHI. I just want to give an example which I think illustrates the point you are making very well. Monday Treasury targeted a service provider for Mahan Air, the IRGC Airline, the airline that carries weapons and personnel to Syria.

The service provider is in Malaysia. It transacts with the airline. Last year, in this committee, I presented a list of 67 service providers that are waiting to be punished for their support, material support to an entity sanctioned under Executive Order 13224.

That is the action that the U.S. Government can take—

Chairman PEARCE. OK. Ms. Rosenberg, wrap it up. I am over my time here. Go ahead and finish your statement if you would.

Ms. ROSENBERG. There is an opportunity by looking further down the value chain. However, if the United States only relies on sanctions, then we will be missing an opportunity because, as has been pointed out before, if institutions are just looking at a sanctions list and making sure that their clients aren't on the list, then we are missing everyone behind those front companies and the broader networks that are conducting the proliferation activity.

Chairman PEARCE. We will try to delve a little bit more into that later in the hearing, but thank you very much.

Mr. Foster, 5 minutes.

Mr. FOSTER. Thank you.

Dr. Ottolenghi, you mentioned rather unambiguously in your testimony that there must be no anonymous companies. Do any of you see any path to success on nonproliferation or prevention of proliferation financing as long as anonymous corporations are allowed. Ms. Rosenberg?

Ms. ROSENBERG. I can speak to that. I think there is an incredible opportunity before you all today to take action on beneficial ownership which will have a direct effect in banning anonymous companies.

And it is through those companies that an array of financial ills occurs through this financial jurisdiction, and the United States as a pace setter, as a standard setter for the entire global community, must lead and demonstrate that anonymity in companies through which proliferation can occur is unacceptable.

Mr. FOSTER. Any other comments on that? Is the logic just that simple?

Mr. OTTOLENGHI. I couldn't agree more. Most of the networks I have studied over the years involving proliferation and money laundering for terror finance all relied on opaque jurisdictions and anonymous companies and beneficial ownership. It is a critical tool for their action. And we should definitely advocate and promote more transparency.

Mr. FOSTER. And which countries besides the United States are going to have to clean up their act on this?

Mr. OTTOLENGHI. A vast number of jurisdictions in the Caribbean Basin are an obvious place to start. Jurisdictions that are under U.S. sovereignty such as the Marshall Islands, jurisdictions in Europe. In small countries like Monaco, Andorra, Lichtenstein. These are places, the British Isles that are not, direct part of the United Kingdom such as the Isle of Man, such as the Channel Islands. All of these are places that are being used and abused for this type of activity.

Ms. ROSENBERG. If I may add to this, there are a handful of countries that have received good marks on beneficial ownership of all of them. Everyone, including those jurisdictions of greatest proliferation concern through which we know proliferation transactions are flowing, has an opportunity, and indeed a national security obligation, to do more to identify the beneficial owners behind corporate structures.

Mr. FOSTER. Yes. And Mr. Albright, what would it take for the United States to get a perfect score? What are the top five ways that we blow our grade?

Mr. ALBRIGHT. In 2017, the United States was number one, so we have a fairly tough standard. They are not fully compliant on FATF recommendations. There is money laundering issues. There are illicit flows of money that are at issue. I think the way the United States can improve in our index is pretty much in the weeds, but it did do the best of any country. And it says that overall—

Mr. FOSTER. We have the highest score despite allowing anonymous shell corporations?

Mr. ALBRIGHT. Those are the kinds of things that would lower the score.

Mr. FOSTER. Right. It seems like that should like blow your score completely.

Mr. ALBRIGHT. Everything is weighted and everything is—there are a lot of parts to this. That is one important aspect. But there are many others. And I think, and I don't want to beat up on the United States because we see much, much worse behavior in most of the world.

The United States, even though it has room for improvement, it is still doing the best and is carrying water for most of the improvements that are sought in countering financial proliferation.

Mr. FOSTER. OK. What country besides the United States do you think gets it the best? If you could say the world should adapt the standards of X, what would X be?

Mr. ALBRIGHT. I think the European Union, those countries tended to rank much better than others.

Mr. FOSTER. Do they allow anonymous shell corporations in the EU?

Mr. ALBRIGHT. I don't know.

Mr. KEATINGE. We have a transparent company registry in the United Kingdom as opposed to the Caribbean islands that were mentioned. I would say, as someone not from these shores, the fact that the U.S. allows such opacity in company ownership does not do the reputation, or at least the message that the United States tries to deliver internationally on illicit finance, does not help that message, get taken on board by countries that can turn and say, but hang on a minute. You have this opacity in the United States.

Mr. FOSTER. Yes. And are anonymous land transactions a big part of the problem? Both in the U.S. and worldwide. Which is something that countries are split on and some allow them and some don't.

Mr. KEATINGE. For illicit finance in general, clearly the ability to own a property in anonymous fashion is a huge problem. It's a huge problem in the United Kingdom and a huge problem elsewhere. Specific to proliferation finance, I don't know the answer to that.

Mr. FOSTER. All right. Thank you.

Chairman PEARCE. The gentleman's time has expired. The Chair now recognizes Mr. Pittenger for 5 minutes.

Mr. PITTENGER. Thank you, Mr. Pearce. I thank each of you for coming today for your expertise. It is very valued and appreciated.

One of the outcomes of the JCPOA was the allowing Iranian Banks through the SWIFT authority to operate. How serious of an outcome is that?

Mr. ALBRIGHT. Yes. I can answer, Emanuele can too. One of the—first the Iranian Banks are tied into illicit procurement networks. By removing the sanctions it also made it much easier for those banks to continue or expand illicit activity.

Mr. PITTENGER. Would re-imposing the element that allowed those banks and preventing them from operating, as they were not able to prior to that agreement. Would that assist in our efforts?

Mr. ALBRIGHT. I think—

Ms. ROSENBERG. I can speak to that. The United States has plans to re-impose sanctions removed on implementation day under the JCPOA. That will involve putting back on the list those Iranian banks that were designated. Having them back on the U.S. SDN list (Specially Designated Nationals and Blocked Persons List) means, and because of the secondary nature of them, any country or company or person anywhere in the world providing material support to those SDN entities will face enforcement actions for violating those sanctions. That has the effect of de-swifting those same banks.

Mr. PITTENGER. Thank you.

Mr. Ottolenghi, you mentioned Uganda and several other countries who are not engaged with us. Let me clarify, was that a mat-

ter of will or the lack of capabilities? I know OTA works with certain countries to help them enhance the capabilities and the financial systems, Egypt, for example, right now is really responding to be very supportive with OTA.

Is our concern out there in the field with other countries and our allies, the lack of interest or the lack of technical capabilities in software?

Mr. OTTOLENGHI. I think it's a mixture of both usually. You will find good political will but lack of capacity in some countries and plenty of capacity and lack of political will in others. And one country that comes to mind where there is capacity, but there is no will, is Turkey.

Mr. PITTENGER. Yes.

Mr. OTTOLENGHI. Turkey is a country where in November 2012, at the height of the sanction regime, Iran had approximately 2,600 companies incorporated through foreign direct investment, many of which linked to the regime. Today that number has skyrocketed to—I quote the exact figure in my written statement I think is around 4,600—

Mr. PITTENGER. Quickly, how many countries do you see out there that given the right capabilities, technology, and software, would they be willing to raise their standards and their collaboration with us? How short are we in the process of fully engaging the willing countries to be supportive in getting the technology they need?

Mr. OTTOLENGHI. Again, I think it is a question of allocation of resources and prioritizing. And the challenge in some of these countries are quite frankly overwhelming. It is not just improving their ability to conduct effective anti-money laundering and counterterrorism compliance in the banks.

It is about better training and providing technology to border controls and customs. The challenge is large and big. And so, I think that it should start from testing the political will of these countries to engage in programs that can improve their ability to enforce sanctions and cooperate better with the United States.

Mr. PITTENGER. We host these forums for partner members. We just had one in Berlin this past week. And we found that private sector is a very important element, the banks, the software companies, and others that have come in and after one such meeting we had in Buenos Aires 100 members of one company were down and became very supportive with Argentina to try to get them up to speed.

And I think what I am trying to determine is how much opportunity do we have out there that OTA could be better engaged with those who want to participate in a stronger way?

Mr. KEATINGE. If I may, we require the private sector to implement these sanctions on our behalf, talking to governments and expecting governments in many of these countries to communicate that effectively to their private sector is frankly, if not a fool's errand, then, extremely difficult to do.

You really need to engage with the banks and others in these countries to bring to their attention what they should be being told by their own governments.

Mr. PITTENGER. Thank you. My time has expired.

Chairman PEARCE. The gentleman's time has expired.

The Chair now recognizes the gentlelady from the neighboring State to New Mexico, to the west, Ms. Sinema for 5 minutes.

Ms. SINEMA. Thank you, Chairman Pearce and thank you to our distinguished witnesses for being with us today.

As residents of a border State, Arizonians are deeply concerned about the national security threats we face. Rogue states and terrorist organizations are developing weapons of mass destruction that threaten our homeland.

Drug cartels like Sinaloa and other international criminal syndicates traffic illegal weapons across our southern border and endanger our communities. We must be tough and smart to combat these threats.

Secure borders and a strong military, enduring and collaborative relationships with our allies, and strategically applied sanctions are all essential tools to keep us safe from the likes of North Korea, ISIS, and other dangerous entities.

We must do more. Cracking down on weapons proliferation is essential to our national security and that is why I worked with Congressman Tipton of Colorado to introduce H.R. 6332, the Improving Strategies to Counter Weapons Proliferation Act.

Our legislation improves the Federal Government's ability to stop the financing of rogue states, transnational criminal organizations, and terrorist groups. Our bill facilitates development of intelligence products that financial institutions, the intelligence community and law enforcement can use to identify and stop transactions linked to weapons proliferation.

We shouldn't let a terrorist organization get away with building a dirty bomb or chemical weapon because our government wasn't using all of the tools at its disposal. And we must do everything possible to keep Arizona families safe.

With that, I have two questions for Ms. Rosenberg with the Center for New American Security. My first question, Ms. Rosenberg. Our bill's reporting requirement improves the types of intelligence products FinCEN offers to financial institutions.

Given your expertise, could you elaborate on the kinds of unique insights that FinCEN has that financial institutions, the intelligence community, and law enforcement might not have on their own?

Ms. ROSENBERG. The information that FinCEN gathers as supplied to it by all manner of reporting institutions, banks, first and foremost among them, money services business, important in border States in particular, brings together information on suspicious activity and cash movements.

And when this information is aggregated in FinCEN and is accessible by the law enforcement community and intelligence community, there is an opportunity to look broadly for trends here. This may include structuring or other activities, the footprint of which you can see for drug cartel activity, for example, or our other illicit activity.

Now, there are plenty of authorities and opportunities for FinCEN to gather this information, to analyze it, for the law enforcement community to do that and to use these intelligence prod-

ucts to go after these concerns in various ways, with sanctions and with law enforcement activity.

But the United States would be in a better position, and FinCEN data would be better, and there will be even more reporting to FinCEN, if there was more disclosure about the entities, the companies that are doing these cash transactions and that are making these wire transactions.

With more information, for example, information that would be generated by the beneficial ownership requirements that this Committee has put forward in draft form in this Congress, in the FinCEN database and accessible to the law enforcement and intelligence community, there would be even better insights.

Ms. SINEMA. Thank you.

My second question is related to legal small arms and light weapons that are trafficked across our southern border. This is a dangerous and persistent problem in my State of Arizona. The flow of these weapons across the border is often carried out by violent drug cartels like the Sinaloa who threaten communities all across our State.

We must be doing more to stop groups like Sinaloa in their cross border trade in humans, drugs, and weapons. How could FinCEN's intelligence products assist law enforcement in cracking down on these drug cartels? And could these intelligence products be useful in helping financial institutions combat structuring, which cartels like Sinaloa use to avoid our current anti-money laundering regime?

Ms. ROSENBERG. You brought up a good point about the cross border money flows related to small arms and other criminal activity across the border. Right now the United States doesn't have a requirement for reporting cross border financial transactions. That's something that Australia and Canada do. And it has been the basis for those countries to track illicit activity, including proliferation finance which is the topic of this hearing today.

The United States could pursue that, and it has been floated. There is a draft rule that has been put out and considered but not taken forward.

That rule would be a huge asset for combating cross border criminal activity including small arms transfers and the money moving with them.

Ms. SINEMA. Thank you so much. Chairman, my time has expired.

Chairman PEARCE. The gentlelady's time has expired. The Chair now recognizes Mr. Rothfus for 5 minutes for questions.

Mr. ROTHFUS. Thank you, Mr. Chairman.

Dr. Ottolenghi, Iran and its terror proxy Hezbollah are currently engaged in hostile or criminal actions around the world and most notably against Israel and her allies. The Trump Administration's decision to withdraw from the JCPOA was wise in my opinion. Before the JCPOA when nuclear related sanctions were in place in Iran, was there an increased awareness on Iran's illicit procurement efforts?

Mr. OTTOLENGHI. Based on my research which is all open source, I can tell you two things. One, that Iran's proliferation networks which preexisted the JCPOA and which, if Iran had intended to

genuinely dismantle it or walk away from its nuclear weapons ambitions and rejoin the international community as a responsible player, those networks would have been dismantled, would have been taken apart, would have been shut down.

We have evidence that none of that happened. That those networks continue to be active and networks that were targeted by sanctions prior to the JCPOA have been reconstituted in some cases. That gives you a sense of the intention.

The second point is that, of course, Iran's proxies have continued and even expanded dramatically their efforts to continue to raise cash through cooperation with criminal cartels across the world from Latin America to West Africa in an effort to finance their terrorism and their military activities in the Middle East.

On both accounts, you can see that the JCPOA has not in any way pushed Iran to become more responsible on either proliferation or terror finance.

Mr. ROTHFUS. Has there been any evidence of Iran seeking illicit goods or technology outside agreed upon channels since JCPOA went to effect in January 2016?

Mr. OTTOLENGHI. By all means, yes, I believe that the latest U.N. report on this matter highlights a number of procurement attempts that were done outside the accepted or the procurement channel organized by the JCPOA.

We are aware of some procurement attempts of what we think is dual use technology. We cannot share it publicly, but I would be happy to brief the members in private. There is by all means plenty of evidence that Iran has continued to seek technology that could be put to use for nefarious purposes.

Mr. ROTHFUS. What impact will President Trump's May 8, 2018 announcement of the exit of the U.S. from the JCPOA have on proliferation financing?

Mr. OTTOLENGHI. I think that you will see as I said the ramped-up attempts by Iran to procure and also to just evade sanctions on a broad front in order to keep its own economy afloat. I think that there are two differences between the situation now, the current situation and the situation before 2006 when the U.N. sanctions regime began and created international consensus for economic pressure against Iran.

The first is that, of course, this time the United States right now does not have the international community going along with it on withdrawing from the JCPOA, but on the other hand, you have 10 years of experience of U.S. secondary sanctions that are very vividly in the mind of the international financial sector, the business community and so on.

And we are seeing already that regardless of steps taken and countermeasures by the European Union or other countries that want to preserve the JCPOA, the vast majority of global business is walking away from Iran because they just do not want to take the risk of finding themselves on the wrong side of U.S. authorities.

Mr. ROTHFUS. A recent staff report from the Permanent Subcommittee on Investigations reveal that contrary to Congressional testimony of Obama-era officials, the U.S. Department of the Treasury authorized a specific license allowing a conversion of $5.7 billion in oil revenue held by Bank Muscat in Omani riyals to

euros, which would necessitate a conversion to the U.S. financial system. What do you make of the Treasury Department's issuance of this license?

Mr. OTTOLENGHI. I really can't speak to this matter or on behalf of the Treasury Department, if any of my colleagues would like to add.

Mr. ROTHFUS. Let me ask you this, despite urging from OFAC, two U.S. banks declined to convert the money, citing compliance and reputational risk, what implications for proliferation finance could such conversion have had?

Again, two U.S. banks declined to convert the money, citing compliance and reputational risk, what implications for proliferation finance could such a conversion had it taken place have had?

Mr. OTTOLENGHI. It would give Iran access to dollars, and the ability to transact in dollars, it would give legitimacy to these types of transactions. The whole purpose of the financial sanctions regime is to deny Iran access to legitimate financial avenues for financial transactions of the global level. The whole idea of deswifting Iran is not so much that you are going to shut down their banks or prevent them from buying and selling, but it is basically pulling the plug on an international platform that allows for millions of transactions and legitimate transactions on a daily basis.

It makes it extremely difficult for Iran to transact, and it makes it easier for financial institutions to avoid being exposed to these types of transactions. When you allow these transactions to go through nevertheless, you expose your financial system to reputational risk.

Chairman PEARCE. The gentleman's time has expired. The Chair now would recognize the gentleman, Mr. Lynch. You have the floor, sir.

Mr. LYNCH. Thank you, Mr. Chairman.

I want to thank the witnesses, very thoughtful testimony. It is ironic though and somewhat counterintuitive, so we talk about these sanctions against Iran, and against Russia, but we allow them, we allow them set up shell corporations in the United States to purchase property, to purchase aircraft, because we don't have any way of telling who owns the property. You have Iranians who have bought high rises in New York City, you have Russian oligarchs that have bought a lot of property in Florida.

And because we refuse, we thump our chests every time we assert sanctions, but the reality of the situation is that we don't know who is buying property here in the United States, we don't have a public registry like the U.K. Is that right, Ms. Rosenberg?

Ms. ROSENBERG. I certainly agree that is an enormous problem. Anonymous companies, and the ability for those transactions you have described to occur, as well as the ability for U.S. financial institutions to bank entities, the beneficial owner or the natural person behind which they are not sure, is an enormous financial crime vulnerability, not just for proliferation finances we are discussing today, but across an array of potential financial criminal activity.

There is a new customer due diligence rule that has just gone live. However, I am concerned by some efforts to slow walk the implementation of that, and you all are poised to encourage its urgent implementation. It is one of the few tools available at present,

given that there is a massive gap in beneficial ownership information, to try and understand who customers of financial institutions are. I would encourage you all to look aggressively at the need to implement it immediately.

Mr. LYNCH. Thank you. Mr. Keatinge. Do you think I would be helpful if the United States as a leader, a global leader, adopted a system where they required people to disclose who they were when they purchased property in the United States or do business here in the United States?

Mr. KEATINGE. Without doubt. I think you have to put yourself in the position of those countries around the world that are visited by U.S. Treasury officials telling them to do certain things in order to strengthen the integrity of the global financial system. And those things that they are being asked to do are absolutely right. But do what I say not what I do, is often the cry.

The other thing I would like to say is when I arrived yesterday, I had to show my passport, United States knew I was coming, I filled out all the forms in advance, to Liz's point, I don't think you know what money is coming into this country, we have the same problem in our own country, and that to me is a national security issue, if you don't know what money is coming this country, you don't know how that money is then going to be used to manipulate this country. Understanding what money is entering your country I think is an important security consideration. Forget money laundering.

Mr. LYNCH. Thank you. I think we are the laggards in this, I was speaking for the United States and our financial system, so you have the U.K., and I think a couple of other countries, Denmark is another one that has a public registry, so you can actually go online and figure out who owns what company or real estate. It is public. And you have 20 other countries in the EU that have committed to adopting this system, so the world is moving toward this more transparent system, but we here in the United States are keeping this nontransparent, this opaque corrupt system, in operation.

I know that Mrs. Maloney has a bill on beneficial ownership. I have one on aircraft because we have a running problem here where we had someone affiliated with Hezbollah that actually registered an aircraft you think after 9/11 we would be concerned about that. But, we have Hezbollah registering aircraft here in the United States because we don't require beneficial ownership.

I love the tough talk about the sanctions, but the fact of the matter is, we are not doing our job to protect the American people and to protect our financial system because we don't require beneficial ownership information when investments and real estate purchases are made here in the United States. I thank you for your testimony and I yield back.

Chairman PEARCE. The gentleman yields back. The Chair now recognizes the gentleman looking for balance in life, that would be Mr. Poliquin. Five minutes. It is not a new quest.

Mr. POLIQUIN. Thank you, Mr. Pearce, very much, I appreciate it. Now, gentlemen, a couple of years ago, the House of Representatives voted strongly against the Iran nuclear deal, I was one of the people who voted against that, it then went over to the Senate, and

never received a vote. I am sure we all recall that deal allowed about $150 billion in cash to be released to the folks that run the Iranian regime. It kept the nuclear arms program intact and this to a country that chants on a regular basis, Death to America.

My question to you and will start with you Mr. Ottolenghi, do you think American families, now we are looking 2 years beyond when that deal was put into effect by the prior Administration, do you think American families are less or more safe today as a result of that deal, and why?

Mr. OTTOLENGHI. A large premise of that deal was that Iran would moderate its behavior and become, over time, a more responsible interlocutor in the region. I think that the evidence is in plain sight that the opposite has happened, as a consequence of releasing resources to the Iranian regime, returning Iran from the cold into the fold of the international community. Iran has become more aggressive in its behavior, in its posture, and it has been allowed to wreak havoc in the region even more so than it did before.

Mr. POLIQUIN. Therefore, we would both conclude that American families are less safe?

Mr. OTTOLENGHI. We are less safe.

Mr. POLIQUIN. Is that correct? And we were also told that if the United States pulled out of that deal, it would be impossible to re-impose sanctions on the country of Iran, is that true? And would those sanctions be effective?

Mr. OTTOLENGHI. The United States doesn't need the rest of the world to have permission to impose or re-impose, expand, elaborate, extend sanctions against Iran. I think that the key will be how credible the threats and the deterrence of sanctions are as we move forward. And for that, you need the Executive Branch to be willing to vigorously enforce sanctions, and punish those who will challenge and violate U.S. law.

Mr. POLIQUIN. Mr. Keatinge, I have introduced a bill in this committee called the Iranian Leaders Asset Transparency Act, you might not be familiar with that. It received a significant bipartisan vote here in the House, and has not gone anywhere in the Senate. It effectively looks at the 70 or 80 individuals that run the Iranian government, whether it be political leaders or military leaders, it requires the United States Treasury Department to post on its website the assets that are held by those 70 to 80 individuals, post them in not only English but the three languages that are practiced in Iran, such that the world can see the assets accumulated illegally in many cases by these individuals and not reaching their people.

Do you think that's a good or a bad idea to show the world how the Iranian people have been ripped off by these folks that chant Death to America?

Mr. KEATING. I think the transparency of asset ownership by any politician, any leader is an important—is an important consideration. The posting of that kind of list, you see the impact that the posting of the list of Russian names had certainly in Europe when the treasury posted that list early in the year, people sat up and took note, OK, are these people likely to be subject to sanction by the United States, we perhaps just stood clear of them and some of them were subsequently sanctioned, but transparency of political

leadership asset ownership anywhere in the world is a critical issue.

Mr. POLIQUIN. Mr. Keatinge, also to continue please, are the demonstrations the best of your ability still continuing in Iran?

Mr. KEATINGE. As reported, yes, but I don't know them in detail.

Mr. POLIQUIN. Anybody have any further—Mr. Albright, any? Ms. Rosenberg? Any idea?

Ms. ROSENBERG. I too read about them in the newspapers. I have no personal knowledge of that.

Mr. POLIQUIN. OK. Thank you very much, Mr. Pearce, I yield back my time. Thank you.

Chairman PEARCE. Thank you. The gentleman's time has expired. The gentleman from North Carolina, Mr. Budd, is recognized for 5 minutes.

Mr. BUDD. Thank you, Mr. Chairman. I want to thank all our witnesses today, and Ms. Rosenberg, I want to give you a special thank you and a shout out for your help through CNAS' assistance with our virtual currency task force legislation H.R. 5036, really appreciate it, so thank you again. And, Ms. Rosenberg, we have financial sanctions on proliferators to stop them from raising and moving money for their nuclear weapons programs. In your own opinion, are these sanctions enough to stop the proliferation finance or is the problem a lack of enforcement of these sanctions?

Ms. ROSENBERG. Thank you for the question and your kind words. They are not enough, sanctions are not enough, and it is not just because there are no sanctions. Surely there's more opportunity to impose more sanctions to expose and go after proliferation activities where it occurs.

But as we were discussing earlier, there is a broader approach toward counter-proliferation activities than just looking at a set of sanctions. It exposes a vulnerability that we have, because if we know as we do, that North Korean proliferators, Iranian proliferators are good at using front companies and shell companies, and trusted agents who change their names, then it is a near impossible task to keep that sanctions list up to date so that we can be sure that we are not providing a means for moving money, for raising money, to proliferators. As the United Nations has pointed out in calling for a broader approach to counter-proliferation activity and counter-proliferation finance, we must look at the nature of the conduct, not just specific entities.

Mr. BUDD. Thank you. If sanctions are not enough, what would you suggest Congress do to counter this threat?

Ms. ROSENBERG. One set of immediate things that Congress can do and that you all are very well placed to do is to take action to promote transparency for companies, for entities that would use the U.S. financial system, not just to prevent proliferation activities moving through the U.S. financial system, and by the way, we know that is occurring, that North Korea has even in the recent past, moved money through the U.S. financial system.

We must safeguard our financial system, and also serve as a standard for other jurisdictions internationally. As Tom was just saying, transparency is our friend here, and that can be accomplished through beneficial ownership legislation, through requiring more information in cross border payments, knowing who brings

what kind of money into this country, and removes it again. And also, in encouraging aggressive implementation of the CDD rule.

Mr. BUDD. I appreciate you are mentioning North Korea. Thank you. And now I will switch over on North Korea, to Mr. Albright. Can you discuss how North Korea most regularly accesses the global financial system? And according to Ms. Rosenberg, even the U.S. system?

Mr. ALBRIGHT. Typically, the North Koreans, if they are going to use banks, they are going to use Chinese banks, I think one of the challenges has been for Administrations to sanction those banks. You can—obviously China is deeply opposed that, but I think—if things don't work out well with North Korea, and it is—and I wouldn't give it a 50/50 chance that they will, namely the negotiation succeed, and I think it is very important for Congress to be willing and prepared to pass even harsher sanctions going after even what Chairman Pearce called going after these secondary, second row of sanctions violators.

And I think there has been legislation that has been drafted and discussed that it could help the game, because in the end it is not just a question of going after entities—the tactics change, countries adapt to the sanctions, so you constantly have to refresh them and think of new ways to improve them. And I think the U.S. Congress and particularly the House of Representatives has been a major leader in coming up with new sanctions approaches that are or have been quite effective.

Mr. BUDD. Thank you, Mr. Albright, just to continue and since you narrowed it down to China and their financial institutions, what do they do to help with North Korea's access to critical components and technology? It is something you have insight into?

Mr. ALBRIGHT. They haven't done enough. It is better than it was a couple years ago, but, the concern now is just that some of the actions China took will diminish—China is their shop—it is North Korea's shopping market, and it is not just Chinese, it is American, German, British, you name it, companies are there. And they are selling goods to China, and the North Koreans are masters at acquiring fairly sensitive goods for their nuclear and missile programs and to be able to exploit China's weak export controls.

Now they did clamp down, and that was a positive sign, but there are some signs that they are weakening, and I think if things don't go well, one of the things that is going to have to be done is to make sure that China understands that it can no longer be a marketplace for the North Korean WMD and missile programs.

Mr. BUDD. Thank you. My time has expired, but before I yield, if you would add in any of your further answers that you are able to, just anything you would suggest to the legislative branch or the Executive Branch that we can do to address some of the shortcomings. Thank you again. I yield back.

Chairman PEARCE. Thank you. And just for those of you still here, it is the Chair's intention to go to a second round and I think that is going to be the focus of the round, so if you can hang around. New Mexico neighbor to the north now, Mr. Tipton, Colorado, is recognized for 5 minutes.

Mr. TIPTON. Thank you, Mr. Pearce. I thank the panel for taking the time to be here. I think we have a pretty evident case lined out,

particularly the doctor had lined out some of the complex webs that we see in terms of being able to create shell corporations, that are going to be able to seek financing, but part of the challenge obviously is when you get those smaller sized corporations, we do get into the financial institutions, that are facing some reputational risk, institutional risk, when it comes to frankly funding illicit firearms and weapons with perhaps not even the knowledge that they are actually doing that.

And that—Ms. Rosenberg, if you maybe speak to really here in the U.S., we have a pretty robust system to be able to identify and counter some of the elicit finance that does go on. But when it comes to our smaller financial institutions, do you believe that there is an actual awareness that exists in some of the contemporary realities that we really face with the proliferation finance, and in the threats that they have?

Ms. ROSENBERG. I should start by saying the United States is best in class when it comes to identifying potential proliferation activities, to analyzing this, to taking law enforcement or sanctions action. But that is not enough. We still witness a North Korean nuclear program that is very dangerous and scary. We must do more even if the United States is best in class.

There are a few institutions that sit atop the best in class status, some of the major U.S. global banks, financial institutions, and corporations have their own financial intelligence units, and are able to proactively look for patterns of proliferation, and communicate that directly to our law enforcement community. We are in their debt, those two constituencies.

However, these smaller companies that you have mentioned or financial institutions, regional credit unions, we have seen in a number of instances, that they don't have the staff, the awareness, or the compliance culture to recognize when certain kinds of financial abuse comes through their system. However, not all of them have direct international relationships, they must go through some of these bigger money center banks in order to conduct international transactions. That becomes a check on their activities, but it is really up to the Federal and State level banking supervisors and regulators to help them to understand and to follow the law and to identify and stop proliferation activity where it may occur and affect them.

Mr. TIPTON. Do you have some direct suggestions along those lines? You had spoken a little bit transparency obviously, and we understand certainly that some of the corresponding banking connectivity that's going to be there, but just being able, some actions that the smaller institutions institutionally could take, or is it simply a matter of scale, size, and dollars?

Ms. ROSENBERG. And understanding risk. The United States has a risk-based approach to its financial supervision, and the Fed, the OCC that oversee the biggest financial institutions and those they supervise have a rock solid understanding of what that looks like. But risk is different for different institutions, of course, there are smaller regional banks in the United States that have much broader exposure to Latin America, for example. Even while they are not the biggest money center banks, they should have a good sense of their risk. Who is coming to Miami? Who is structuring trans-

actions in the United States and buying anonymously real estate in that market?

Understanding their risk well, is up to their regulators at the State level. Federal regulations can help them calibrate their risk appropriately. We should emphasize that banks must understand the particular risk they have with their footprint and their orientation for financial activities. It is different for every financial institution.

Mr. TIPTON. Would you maybe share with us a couple of your thoughts. Just focus a little bit on the SARS (suspicious activity report) reports that American banks are required to be able to submit to FinCEN and do you think we have sufficient information about how the SARs reports are used by law enforcement, to be able to combat proliferation financing?

Ms. ROSENBERG. Do you have sufficient information? I don't know what kind of briefings that FinCEN gives to you, I would encourage you to have a full and frank conversation with them. It is not just them, because they administer the BSA (Bank Secrecy Act) and collect BSA data, and I think any law enforcement officer looking at terrorism finance or proliferation finance might take issue that these SARS are FinCEN SARs. They belong to the entire law enforcement and intelligence community, and they should be empowered to have access to them and to use them.

Mr. TIPTON. This can probably just be a yes or no, but do you think it would be helpful to know more about what kind of suspicious activity reports, what they use the actions for when the reports are made?

Ms. ROSENBERG. Yes, on proliferation finance, because it will signal to them that you care, it will give a demand signal to them, and the financial institutions that they oversee, that must submit the SARs to know that this is a priority, that they must look for and take action on.

Mr. TIPTON. Great. Thank you and my time is expired. Thank you, Mr. Pearce.

Chairman PEARCE. The gentleman's time has expired. Now, before I recognize Mr. Davidson, I would like to inquire our panels if you are able to stay around for a second round, does your time allow that? Also, in direct for us as members, of what I am going to do on this next round. What I am going to do on this next round after, we are going to take the two more with five questions each? And then I think there is a consensus among the minority and majority that we would really like to hear from you specific suggestions.

And so we are going to go through, one, two, three, four, with one specific. And if your specific it sort of general and not picking on you Mr. Rosenberg, but you said, if we were going to do something, it has to be on transparency, then give us two things on transparency. I will give you one big item and two sub items.

And then I would like the questions to delve into this where we see from a policymaker's point of view what it is that these experts are suggesting that we do if we want to ratchet up the pressure on this financing of weapons of mass destruction one or two notches, we can reach for the sky, but it is not going to happen between now and the end of the year.

We might get a specific bill with specific recommendations that is lightning quick, and if you have one chance to do something before the session ends, what would you do, so that's where we are going after the two or 5 minutes here. Please be prepared, you have to be concise, we have a vote series coming up.

Mr. Davidson, make it a good 5 minutes, sir.

Mr. DAVIDSON. Thank you, chairman. Thank you for our witnesses, and Mr. Albright, it is great to have an Ohio-educated Wright State grad in the room which is not in the district, but adjacent and Oberlin also a great Ohio education system. And I assume the rest of you by your resumes are all sufficiently well-educated as well.

Thanks for your expertise in the matter, but I want to spend a little bit of time specifically to deal with Iran, and the threat of weapons of mass destruction, weapons proliferation in Iran, but also how they might deploy them. Under the previous Administration, as part of negotiating the JCPOA, there was Operation Cassandra, activities involving fundraising, potentially other activities, and I just wonder if—I apologize for the potential error in your name, Mr. Ottolenghi, could you address that?

Mr. OTTOLENGHI. Absolutely. The, Iran remains the main sponsor financially of Hezbollah, but over the past decade or so, Hezbollah's budget has grown exponentially and dramatically for its needs because of its involvement in Syria after 2011, because of its obligation to reconstruct the destroyed south of Lebanon after the war in 2006, while Iran's contribution has become unreliable due to the increased pressure of sanctions.

Hezbollah has developed networks and cooperation with criminal syndicates across the globe to finance these activities through this type of convergence. Narco-terrorism is the word most commonly used. This activity is yielding, in our conservative estimate that I have based on open source research done by some of my colleagues, to about $300 million a year, out of an estimated budget of about a billion dollars a year.

People who were involved in the Project Cassandra over a decade would probably estimate that the contribution to Hezbollah's finances through these type of illicit activities is dramatically larger. We are talking about a global criminal syndicate that cooperates with local criminal syndicates, affecting the security and the wellbeing of our societies this is not just a national security issue, it is about our neighborhoods and our lifestyle, and the safety of society.

Mr. DAVIDSON. If we look at how they are doing this, not just what they are doing, how much of this is conventional movement of money, wire transfers and whatnot between Iran and proxy groups and how much is moved by Hawala networks or cash?

Mr. OTTOLENGHI. I don't have accurate estimates, but I can say based on my research that a significant part of these funding activities go through trade-based money laundering that is conducted through front companies, transacting through or with the assistance of regular banking institutions, money exchange houses, but it is mostly wired into the formal global financial system. And a lot of it goes through the United States.

Mr. DAVIDSON. Thank you.

Mr. Albright, one of the things that we are wrestling with is because of these front companies, knowing the beneficial ownership and if all this data was used for good purposes to only catch criminals, there would still be a burden of who has to collect it and monitor it. In the current system the government has effectively nationalized parts of our banks and commissioned them as law enforcement officers to collect lots of data.

While this data is very valuable for national security, some approaches would have the burden shifted from banks out to every company that there is reporting requirements, that they fill out every year, over and above the other forms and documents that they fill out every year.

What is your best recommendation as we prepare to transition into? How might we best know the beneficial ownership of corporations and balancing the right to privacy that is perhaps unique to America because of the fourth amendment?

Mr. ALBRIGHT. I think that transparency is important and it has been discussed, better than I can do, by other witnesses. I would add though that we don't have a good system here for companies to report like banks do. There are all kinds of suspicious transactions that occur and the system has not been established here, as in let us say in Britain and Germany, for companies to easily pass on those suspicious reports.

FBI, ICE do a great job of collecting things, but we don't have a routine system like the SAR system—

Mr. DAVIDSON. Where we do for banks. Thank you and valid point. Hopefully that informs our debate going forward and my time is expired.

I yield, chairman.

Chairman PEARCE. The gentleman's time is expired.

The Chair now recognizes Mr. Emmer for 5 minutes.

Mr. EMMER. Thank you, good Chair. Thanks to the panel. Following up on where my colleague and my friend, Mr. Davidson was headed, I have major concerns even though the area that we are trying to address today is incredibly important to our national security, I think you can become a prisoner of your need for security, and I really am troubled at the tone that suggests that U.S. citizens should give up more of their privacy rights and the private entities and my colleague just said banks being nationalized as part of the Federal law enforcement.

They do. They become an extension of Federal law enforcement activities. And it sounds even from the panel at times as though the United States is a problem when in fact this is about third-party facilitators. This is about countries and entities in other countries that are breaking the law and we need to focus on them and figure out how we stop them from doing that. The best example was North Korea earlier. The problem isn't North Korea. We know North Korea is going to break the law. The problem is China or anyone that would aid North Korea in that activity.

I am not saying that I am adamantly opposed to doing certain things on our end. But it seems to me that should be the secondary phase. The focus should be on those that are committed to breaking the law, supporting international criminals, crime networks, terrorists and the proliferation issue that we are talking about.

Ms. Rosenberg, I think somebody commented or started to go into this a little earlier, do you believe that our banks currently understand the contemporary realities of the proliferation, late in the day, finance threats that they face?

Ms. ROSENBERG. Thank you for the question. A number of the big U.S. and biggest global banks certainly understand the nature of the threat. And what should be concerning to us is that even when they understand it, they know that they may be incapable of getting after it.

They may be asked by a client to host a set of transactions, and will look at a particular customer, or host or facilitate a lot of shipping transactions. They may be given a list by the U.S. Coast Guard of vessels that may be involved in illegal ship-to-ship transfers, and have to make a decision about whether they should provide services to the shipping agent or the flagging registry.

What decision are they to make? They have inadequate information about potential proliferation activity. That is the concerning part. Even the people who know that they have inaccurate information, which is to say nothing about those who are committed to breaking the law and are utterly unconcerned about facilitating proliferation activities.

Mr. EMMER. Right. That goes to the next question which I think the chairman touched on a little bit early in this questioning and it goes to what you just talked about. They are given a list by U.S. Customs.

If banks screen against sanctions lists, not necessarily the type that you just said, but that could be included, I suppose, does that put them in a position to understand whether or not proliferation is—that they are involved or is that the whole topic of this hearing is that they can't be sure that is what they are dealing with? Does that make sense?

Ms. ROSENBERG. Yes. Perhaps, let me put it this way: All major global banks, not just U.S. banks, major regional banks as well, adopt sanctions lists from the United States, United Nations, et cetera. They are screening transactions against this list.

If they get a hit and it is a known proliferator, they could realistically assume that they have a much bigger problem than one person who tripped.

And even if they say understanding their obligation is not to provide material support to that entity and close their account, they may know that person will go down the road and open an account at the next bank.

They are aware of the problem. They have some limited tools and certain jurisdictions where these banks are prevented from talking to one another about proliferation activity they notice in their own ledger of accounts, that is a problem.

Mr. EMMER. Wow. That is a great point and I was going to ask you because it would have led in to the next question. What are the gaps in the financial institutions' responses to counter-proliferation finance? But I have ran out of time and perhaps after the hearing, we can follow up with the panelists. I really appreciate it. I yield back.

Chairman PEARCE. The gentleman yields back.

OK. We are going to shift the process just a bit here. You see the hustle over in the corner there. Each one of you are going to get one statement up there, OK? It needs to be tight. You are going to put your statement up there. If it is a general statement like transparency, then, you are going to have an A and a B under it, fair enough? And then, we are going to try to probe that from this side because we are the ones that have to try to figure out the policy. You all know the process and you know everything.

We are just trying to take a great, big leap today. We are running out of legislative time in the year. If we are going to do anything in this year almost it has to be very quick. We are just going to go right down the row.

Mr. Albright? And this is going to be much more open here, not the 5 minutes. If you have questions from this end, then, flag me and let me know. But let us get the statements up there. Mr. Albright, what would your statement be?

Mr. ALBRIGHT. Alright.

Chairman PEARCE. And Molly is going to keep with every—

Mr. ALBRIGHT. I would say first of all, the Government, the Congress should require a report from the Executive Branch on revising the reporting, like under SARs, how to educate the banks if they don't understand the goods. But again, they are—am I speaking too quickly?

Chairman PEARCE. Yes. Help her out—help get the text exactly right up here. We are taking steps that would generally take us weeks to get this done. OK.

Mr. ALBRIGHT. Review SARs and other reporting requirements by financial institutions and develop methods for banks to better understand the strategies being used by illicit networks and the goods that are being sought.

Chairman PEARCE. Right.

Has that got you close enough with the script? Get this a little bit bigger just the font, if you can over there. We are going to let you come back—OK, there we go. And you can read it right behind you if you want.

Mr. ALBRIGHT. The SARs, what is in the SARs? An example would be—I don't think there is a box on SARs where you check that there is suspected activity related to proliferation.

Chairman PEARCE. Make sure we have it right, we will come back and tighten it up after we get everybody and generalized.

Are we ready to move on to the second one? Molly, are you ready to go?

Kristine, excuse me. Kristine, excuse me, I am getting mixed up here.

Mr. Keatinge, are you ready to go on your statement?

Mr. KEATINGE. I would suggest that the right body—you have to apologize, my knowledge of your system is not as it should be. You have Section 314(a) and 314(b) of the USA PATRIOT Act, which allows for information sharing from the public sector, the Government, to the private sector. We should be seeing that actively used to share information with the private sector such that they can actually understand the threat that they are trying to counter. Information sharing needs to be the cornerstone of this initiative.

Chairman PEARCE. OK. Let her catch up.

Mr. KEATINGE. Sorry.

Chairman PEARCE. Let us—somebody help out down there. That is 314(a) and (b).

Mr. KEATINGE. 314(a) and (b) of the PATRIOT Act.

Chairman PEARCE. To be used more actively and you had much more descriptive language there. Go ahead.

Mr. KEATINGE. To ensure that the financial system is able to combat the threat of proliferation finance.

Chairman PEARCE. All right. Mr. Davidson, I expect the question here in a minute, but we are going to get all four. OK. You are going to see the process playing out.

Mr. Ottolenghi, now, tell me again what—you just passed some significant roadblock or some hurdle in your quest for permanent status here. Tell us what that is and we are going to give you a big round of applause here.

Mr. OTTOLENGHI. It is commonly called the green card.

Chairman PEARCE. Yes. OK, all right.

Mr. OTTOLENGHI. It came yesterday.

Chairman PEARCE. Congratulations.

Mr. OTTOLENGHI. Thank you.

Chairman PEARCE. Thanks for working through that and we appreciate you being here.

Mr. OTTOLENGHI. It is an honor and it is an honor and a privilege to have it.

Chairman PEARCE. We thank you. All right, what is your statement?

Mr. OTTOLENGHI. My statement is that the United States should address urgently Iran's abuse of foreign passports by denying access to the visa waiver program to any country that sells its citizenship for investments. And it could make exceptions if countries are willing to share on an ongoing basis names and due diligence packages done on those to whom they sold their passports.

This is a technique that the Iranians have used in order to evade sanctions, establish front companies. It speaks again to the issue of transparency and I think that by leveraging this tool, the United States would devalue this program or discourage people—

Chairman PEARCE. She is running a little bit behind you. These Italian guys, they run fast. Take a look at the script and tell her what you need to fill in and look behind you if you can't see it. You have the script here behind you and on the side. Take a look and see what we need to get to catch your idea completely.

Mr. OTTOLENGHI. Yes. The United States should address Iran's abuse of foreign passports by denying access to the visa waiver program, the program that allows people to apply for a visa electronically.

Chairman PEARCE. Yes. Any country that allows—

Mr. OTTOLENGHI. Any country that sells its citizenship.

Chairman PEARCE. Yes. Iran would be the main focus, but any country that does this, that sells or facilitates the illegal use of passports should be denied access to the visa waiver program or any other—

Mr. OTTOLENGHI. No. No, not the illegal use, but that they sell their citizenship through investment programs.

In other words, people who instead of taking up residency like I just did, just bring money in and in exchange, within a matter of weeks or months become citizens of that country.

Mr. FOSTER. Could you give us a brief list of the countries that currently do that?

Mr. OTTOLENGHI. There are a number of Caribbean nations. The best known ones are Saint Kitts and Nevis which were actually the target of a FinCEN advisory in May 2014 and the advisory spoke to the fact that this program was being abused by Iranian citizens with the purpose of evading sanctions.

Other countries in the region, the Republic of Dominica, Antigua and Barbuda, Saint Lucia, but also other countries including Malta, a member of the European Union which has recently created an investment program to give people citizenship. And it has become the center of a very dramatic case involving money laundering for Iran by an Iranian national with a Saint Kitts and Nevis passport that was recently detained at Dallas International Airport upon coming into the country in March 2018.

Chairman PEARCE. OK.

OK. We need to—Ms. Rosenberg.

Ms. ROSENBERG. Mr. Pearce, in your bill, H.R. 6068, Section 10, please transform the study requirement on beneficial ownership to a binding requirement to collect and report beneficial ownership in the corporate formation process.

Chairman PEARCE. OK.

Did you get it, Kristine?

Mr. FOSTER. This would be as the corporations are established or on an ongoing basis with the duty to report any change?

Ms. ROSENBERG. I would love both.

Chairman PEARCE. And by the way, we are in deep in discussion today after talking to Secretary Mnuchin on that one section of the bill to make it much tighter, but that is—OK, so, now I would like for each of you four to take a look and if you want to, we just got them in random order. If you agree that any of these should be placed at the top of the list, that you look at someone else's statement and think that should be at the top of the list, I would like for you all to reorient those now and then we are going to go kind of questions from up here.

Mr. ALBRIGHT. Can we edit ours?

Chairman PEARCE. Say again.

Mr. ALBRIGHT. Can we edit them or should we do that after?

Chairman PEARCE. Yes, please do. Yes. Edit and this is the time where you should really get it more accurate. It is the reason we are putting them up here exactly for that reason. Yes.

Mr. ALBRIGHT. Alright—

Chairman PEARCE. Kristine, can you follow what they are saying there.

Mr. ALBRIGHT. Executive branch to review the information sought in the SARs.

Chairman PEARCE. Sought, S-O-U-G-H-T. Sorry.

Mr. ALBRIGHT. Yes, sought in the SARs from banks and other FIs. And how to more effectively—and then, so, how to more effectively educate FIs to better understand.

Chairman PEARCE. Alright. Any other—this is precisely the reason we got here because again this process would take weeks, trust me between you all and us, just the way it works.

Any other amendments, anybody want to tighten it up? Do you want to amend it?

Ms. ROSENBERG. I will amend briefly.

Chairman PEARCE. Sure.

Ms. ROSENBERG. I will take your excellent suggestion, Mr. Ranking Member, and add not just upon incorporation but let us be sure that we are following it on a continuing basis, so, evaluating beneficial ownership.

Chairman PEARCE. All right. Kristine, are you getting that?

Ms. ROSENBERG. Thank you.

Chairman PEARCE. Make sure we got it. Is that good?

Mr. FOSTER. Yes. I think there is a grammar problem. You can put "and on a continuing basis".

Chairman PEARCE. Yes. Right, which articles of corporation for a small company can change tomorrow? My wife owns the company and when we bought it, we changed from complete ownership here to one person to us. And if it is not on an ongoing basis, then, we have not done it.

Alright, so, everybody comfortable here?

Alright, Mr. Davidson, I know you already have a question on 314(a) and (b). Ask the question, push just a light bit, sir.

Mr. DAVIDSON. Yes, so, 314(a) and (b) and the PATRIOT Act really stretched the bounds of U.S. privacy protections, not something that the U.K. seems to enjoy or appreciate much. But, I can appreciate from the intelligence gathering perspective why we would want to share this information.

But, let me illustrate some of the activities that happened in the U.S. and how do we get this balance right in your estimation. The safeguards are important. Under the previous Administration, there were reputational risk directives given by regulators that said we really don't think you should bank with this company because they sell weapons or something, which is perfectly legal in the United States, but not appreciated by the previous Administration.

Companies that had strong balance sheets were told that because of reputational risk, we can't bank you. That meant that they lost access to that bank. Once you start sharing all the information across the market, these are law abiding companies that could face a scenario where they are not just locked out of their current bank. They are locked out of the U.S. banking system. When we are targeting illicit finance, we want these people to be locked out of the U.S. system to the extent that we want to block their actions from happening and we want them to use the U.S. financial system so that we can actually detect their activities.

There is a paradox there. How do we get this right and protect the things that we established and supported in the PATRIOT Act while protecting our founding documents and principles?

Mr. KEATINGE. The issue of de-risking that you refer to is something that I have studied extensively and it is not just weapons companies. It is charities, money service businesses, et cetera, et cetera. At the heart of much of the de-risking and I don't know the

case you refer to, but at the heart of much of the de-risking is a lack of knowledge and understanding on the part of the banking system.

Charities are a risk, OK? We get rid of all charities. What about if you were told charities X, Y, and Z for this demonstrated reason are a risk? OK. Then, we don't get rid of all charities. We just get rid of charity X, Y, and Z.

We have something in the United Kingdom called the Joint Money Laundering Intelligence Taskforce which is a taskforce where banks and the Government sit together and talk about financial crime risk in a way that makes the financial system in the U.K. understand the nature of the risk that the Government sees, that the authorities see in a more effective way than simply just saying "We are not going to deal with anybody from country X or country Y."

The risk that you point out isn't entirely fair risk, but that is why this has to be done as a partnership rather than just a direction from the State to say, "This company blank is bad." Why is it that company X or company Y presents a risk? And the way that I would categorize this is that historically, the financial system and Governments have operated a parent-child relationship. Thou shall not file a suspicious activity report and you won't get any feedback, by the way.

OK. We have to continue to have that relationship, but there is also a partnership relationship which needs to be developed. And for the complex, challenging issues like proliferation finance, we will fail until we embrace partnership, because the banks will never be able to solve this on their own. Channels for sharing information in the appropriate way should be encouraged so that we don't get this blanket knee-jerk reaction such as de-risking.

Chairman PEARCE. Mr. Foster.

Mr. ALBRIGHT. Can I add to this? Because, actually in the commodity world it is the same problem. If you just go through and check, do your corporate compliance responsibilities, if you just go and do it by a sanctions list, you may meet the letter of the law but you are not going to accomplish anything. You need to have to apply some intelligence to it internally and that is often missing in the banks.

But, unfortunately, what complicates it here is that—and you see it also in the commodity side—is that the United States system puts roadblocks in the way of Government intelligence sharing and that doesn't exist in Britain, doesn't exist in Germany.

Chairman PEARCE. OK.

Mr. ALBRIGHT. A system I am much more familiar with.

Chairman PEARCE. Let us move to Mr. Foster and then if you can hold that comment—

Mr. ALBRIGHT. And then, so, if you need to change the law to allow—and from the reports we get from the U.S. intelligence community that you have to change the law to more mandate the intelligence community to share information with commercial industry on these key kinds of non-proliferation questions.

Chairman PEARCE. Mr. Foster. Thanks.

Mr. FOSTER. Yes. This is something that we actually get into in the whole issue of the consolidated audit trail on a related thing

which in its eventual plan will have beneficial owner identified behind every stock trade that is made, which there are sorts of interesting money laundering strategies having to do with international stock trades where you agree to lose money in this market and win money in this market in a different country, and very complicated things are possible and maybe even being done.

And the only way that the regulators are able to imagine dealing with that is to have in the fullness of time for every completed trade and in fact, every bid and offer, the beneficial owner identified behind that, and moreover, only the regulator that sees everything can net it out. You can't ask one broker to identify whether or not there is some weird manipulation going on based on the fraction of the data they see.

Similarly, a bank may see completely legitimate operations from everything that they can see and not know that the prices are bogus for the goods that are being traded. And so, ultimately, if you have to solve this problem, it gets more and more intrusive.

And so, my question—the only system that you can write down that you know will work is that the Government sees every financial transaction in the place, which smells a lot like China, where certainly on the commercial side, where everyone pays by cellphone and everyone assumes the Government sees every dime that is spent by consumers in China.

And we seem to be—when you try to write a system that might work, you rampantly are led down that road. There has to be some single entity that can run massive software because no set of humans could do this—massive software to look for patterns of suspicious activity and they have to have access to everything from all countries. And, boy, that scares me.

Is there any way out of that conundrum or is that really the only system that will eventually work?

Mr. ALBRIGHT. I think there is a way. I think—again, I don't want to oversell it, but I know on the idea of Government industry cooperation, one way around that is to actually have it. This in our country, it is much too dominated by police officers whether FBI are showing up with handcuffs in their pocket and they are the ones having the discussion with the banks or the companies and it is intimidating.

It should be the intelligence system. It can be, I hate to use the word, a front. We want to get around some of the quirks of our system. And you want to have a discussion between our best intelligence people and the people who are dealing with the financial system and also with the goods that these—and that gets around a lot of this. And I think Britain has done an excellent job on this and I don't think they are—

Mr. FOSTER. But in Britain, does the Government have access to all financial transactions if it wants to see them?

Mr. KEATINGE. No. No. It doesn't. Obviously—

Mr. FOSTER. There is a *de minimis* threshold. And so, how do you avoid large numbers of *de minimis* threshold under *de minimis* threshold type transactions for example unless you—someone has to add them up.

Mr. KEATINGE. The way the U.K. is trying to develop this is by involving the financial sector in discussions around certain forms

of threat, whether it is human trafficking, terrorist finance, whatever it might be, educating the financial sector on what to look for. And then, wanting them to go back into their systems and say, "Right, given this information, this understanding, guidance we have been given by law enforcement or by intelligence services, now, let us interrogate our data ourselves."

They are not handing over all the transactions undertaken by one of the big banks. They are being guided.

Mr. FOSTER. This is a huge burden. You don't have small banks, but we do here.

Mr. KEATINGE. We do. We have small banks. Don't worry.

Mr. FOSTER. OK. Wouldn't this be just a colossal burden that every transaction, they have to say, "Might this be some weird flavor of dual use goods that we are unaware of?" Do they have to have someone trained in dual use technology at every small bank?

Mr. KEATINGE. The system that we have created over the last 25 years or so puts a huge burden on the banks, on all banks full stop. We would not create the system that we have today if we started with a blank sheet of paper today. The way I think we are trying to address that as I say is by making the assessments risk-based, so, don't spend all your time trying to find everything all the time.

Focus on this particular area, this particular theme, this lead and that is what we are trying to do in the U.K. through this thing, the Joint Money Laundering Intelligence Taskforce, just trying to empower the banking system to be smarter at interpreting their own data themselves.

Chairman PEARCE. Ms. Rosenberg.

Ms. ROSENBERG. If I may offer a comment following up to this and it comes through the theme we have been discussing and to your question.

Chairman PEARCE. On 314(a) and (b), yes.

Ms. ROSENBERG. Right, on information sharing, if you will. There are some bright spots of partnership in the United States. If I may just offer a note of praise to your legislation, Mr. Pearce, prioritizing the financial criminal threats. That is an excellent innovation in our current system and it will help get better at evaluating risk and understanding what are the supervisory priorities, what is the risk.

To the issue about information sharing, I would like to offer some praise for the outstanding work of TFOS at the FBI working on terrorism financing in the United States. They have managed in what is legitimately a fairly chilly relationship between regulated financial entities in the United States and the regulators to bridge a number of divides, to have excellent working relationships with financial institutions and with the intelligence community in order to speak together and gather information pursuant to terrorist threats, Orlando, San Bernardino, Las Vegas, ones that affect us here at home, foreign fighters that also affect us, and security concerns outside our borders.

And they have managed to pioneer a unique relationship in our financial system, in our law enforcement community, where they are able to use official subpoenas and official tools to gather information and also relationships of trust and constructive exchange between these constituencies to do excellent work.

I hope that model can be used also in the counter-proliferation sphere, where WMD folks work on that issue in the law enforcement community and others. This is a bright example I think we should hold up and praise and try to see emulated elsewhere in the law enforcement community.

Chairman PEARCE. OK.

Mr. Davidson.

Mr. DAVIDSON. Yes. Thank you and thanks for the note. I am glad that you called some attention to and praise for our existing law enforcement folks whether they are in Treasury or Department of Justice or Homeland Security. We have had some really great capabilities and by and large, these people are there doing the right things and looking for better tools to be effective in it.

And frankly, the banks, it is amazing to me how enthusiastic they have been about trying to help with national security. Certainly, they do have true reputational risk and some fraud that they want to protect, but a lot of it is just genuine desire to make sure that they help the cause of securing our country.

I guess, to Mr. Foster, I think you highlighted the point that where the state of technology and everything is, to truly know what is going on. If you really wanted to write good algorithms, you would probably want to know every transaction and who is the beneficial owner of every transaction. We are doing it with stocks with the consolidated audit trail. We could easily do it with everything else as long as it is not cash.

If it is digital, it theoretically could be done. And at this point, you have pushed "We have to collaborate more with the banks. We have to collaborate more with the banks." And if they don't collaborate sufficiently enough, now, they really have reputational risk. You are not being good deputies, OK? And we are not here yet and in many cases though, we have approached it. If you think about where the logical end of this might be, it is almost like the Government is actually putting brownshirts into the organization and when the bank needs some more, they just call up and send more brownshirts in. That is where we could go to.

Why not just let the Government operate it? It is such a synergistic partnership. It is approaching other ideologies that the world is seeing become very abusive that we have tried to use civil liberties to protect against and in the U.S., the bill of rights is that bulwark. I guess that is the Pandora's Box we are all reluctant to. And the premise that as you highlighted in 6068, the base language that we are going to criminalize every—the least sophisticated businesses, less than $5 million in revenue, less than 20 employees, if they don't fill out this form, if you changed companies and you added a new shareholder, you didn't go get permission from the Government—or, not really permission, just disclosure. But then, it turns into permission.

This is a system we have worked hard in America to reject and help the world reject and it seems in the name of security, we are trading away an awful lot of liberty and I guess that is the concern. Hopefully, we get it right. I appreciate your input and I think you added a lot to some of that dialog. We will probably have it offline with some of the—

Mr. ALBRIGHT. Can I add—can I respond in some ways to it because—

Chairman PEARCE. Yes, please do.

Mr. ALBRIGHT. I have been involved in trying to set up big data systems at the Department of Homeland Security on querying essentially U.S. exports. We have hundreds of millions that have to be queried and you set up big data systems to try to understand it better and ferret out illicit networks. One has an acronym of BEEP.

The problem in the banks is that I don't think you could do what you are most fearful of. I don't think you could digitize and assess all the banking information that is taking place. The numbers are just too vast. Maybe if there is—in the future, maybe that is possible. But I think that what you mentioned about being a good citizen I think is the driver and should be the driver, that the banks want to be good citizens fundamentally and are willing to voluntarily or meet the requirements of the law to provide certain information.

I think it is the job of the Government to make sure that information is what is really needed and to be able to guide the banks on how to do the searches. That is part of the problem is the banks don't know how to do these searches. And I think it is the responsibility of the Government to step in and try to help resolve that, essentially, that search problem. And cooperation I think is the key, not getting more data because I don't think in the Government we can actually process it in an effective manner. It is so much.

Chairman PEARCE. Mr. Budd, do you have a question?

Mr. BUDD. I just want to elaborate a little bit on Mr. Albright. Number one, we have the banks very concerned about the SARs and how much information and compliance cost that they have. With this potential review, one of the problems with the banks is that they are so demoralized by having to put all this information in the system and comply with it, but they don't know if it actually does anything.

Would the banks be a part of this? Would they understand? Would they narrow it down? Would they change the SARs to make the banks know that they are actually accomplishing a mission here?

Mr. ALBRIGHT. Yes. And I think you certainly would want to talk to the banks a lot about this about what is in their mind is useful. In a sense, they are the first line of defense and they understand criminal activity, non-ethical activity. And so, they are—

Mr. BUDD. Let me interrupt. The SARs actually—are there other questions that you think would be better on the SARs or does it need an overhaul?

Mr. ALBRIGHT. One is—and again, I am not—I don't know. I haven't confirmed this, but I am reading from a colleague's article that there is no check box on the SARs if the banks suspect the activity is related to proliferation.

When we think that for what we are talking about, that would be a critical check box and that would educate the companies, too, of what to look for. I also think there has to be some give and take. Our system has such levels of classification. I know it is hard.

Mr. BUDD. True.

Mr. ALBRIGHT. But there has to be a way to tell the banks who in a sense the bad guys are and how are they operating today, a lot of times, these lists are how they operated yesterday, not today and I think you have to find a way to share the intelligence information in real-time so these banks then become better lookouts and a better frontline of defense.

Mr. BUDD. We are essentially telling the banks how to comply.

I am sorry, Mr. Pearce, but we tell them how to comply, but does that compliance lead to us catching more bad guys? I don't know. That is something we should certainly take a look at.

Chairman PEARCE. But at the end of the day, it looks like that there is a fairly large consensus that some form of beneficial ownership actually needs to be reported. We have to solve that problem among us here, among us policymakers here. I think that probably is going to begin to address in the largest way possible this financing of threats that come through weapons of mass destruction or whatever the process is of breaking the sanctions. Again, a very thorny problem, but we are dedicated to it.

I very much appreciate you spending the extra time with us and addressing these extra questions. I appreciate the focus here to give us really good talking points for this second round of questions. Thank you again for your time and for your testimony 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.

This hearing is adjourned.

[Whereupon, at 4:10 p.m., the subcommittee was adjourned.]

A P P E N D I X

July 12, 2018

Testimony[1] of David Albright before the Subcommittee on Terrorism and Illicit Finance of the House Financial Services Committee

Countering the Financial Networks of Weapons Proliferation

July 12, 2018

A mission of the Institute for Science and International Security is to work to prevent the proliferation of weapons of mass destruction and the wherewithal to make them. As part of this mission, since the Institute was founded 25 years ago, we have focused on detecting, understanding, and characterizing the trafficking of commodities that can be used in sensitive weapons programs with an emphasis on nuclear-related commodity trafficking, also known as illicit trade. In addition to dozens of case studies, reports on our website, and books analyzing such illicit procurement schemes, my Institute recently published a report ranking the export control systems of 200 countries, territories, and entities. This report, the *Peddling Peril Index (PPI),*[2] is the first comprehensive and in-depth ranking of countries' national strategic export controls. In the index, we rank countries based on their capabilities and performance in five areas, which we call super criteria: International Commitment, Legislation, Ability to Monitor and Detect Strategic Trade, Ability to Prevent Proliferation Financing, and Enforcement. Several related publications can be found on the Institute's website.[3]

Preventing proliferation financing, or Financing of Proliferation (FoP), albeit not a traditional component of a review of national export control systems, is one of the most important aspects for detecting and stopping exports of sensitive goods. Our research revealed that countries' ability to prevent proliferation financing is one of the counterproliferation areas most in need of improvement globally and would benefit significantly from a closer integration with export controls.

---

[1] This testimony is the collective work of the Institute for Science and International Security, in particular the work of David Albright, Sarah Burkhard, Ramya Ramjee, Naomi Silverstein, and Andrea Stricker.

[2] "How to Obtain the Book," Institute for Science and International Security, http://isis-online.org/ppi/detail/obtain-the-book/

[3] For more information and additional PPI studies, see: http://www.isis-online.org/ppi

Under the super criterion, *Ability to Prevent Proliferation Financing*, the Institute attempted to measure countries' susceptibility to being exploited or involved in FoP, including violations of international sanctions. The methodology we use is outlined in the appendix to this testimony and is contained in the book *Peddling Peril Index 2017*. For this hearing, we have updated our 2017 FoP results on a preliminary basis and included both the results for 2017 and 2018 here. The final 2018 analysis will not be issued until later this year but enough has changed to warrant the inclusion of this preliminary update.

In the Institute's PPI ranking, the proliferation financing super criterion is the one under which countries collectively performed the worst. Moreover, this super criterion offers the fewest sub-criteria for measuring countries' performance because of a lack of available data and public discourse on the topic, including a paucity of organizations that conduct training in countries that need improvement.

To develop a numerical ranking of performance under the super criterion *Ability to Prevent Proliferation Financing,* countries received points based on sub-criteria that assess countries' capabilities to prevent money laundering and FoP. These sub-criteria are based on their financial regulatory systems and counter-illicit financing programs, for which the main source of data for the PPI is the Financial Action Task Force (FATF). In particular, our starting point was FATF's Mutual Evaluation and follow-up reports on countries' compliance with Anti-Money Laundering (AML) and Countering the Financing of Terrorism (CFT) recommendations. Early in our process, we brought in experts with knowledge of FoP to advise the project on the most effective way to evaluate the FATF-collected data to draw out information relevant to an evaluation of proliferation financing. To supplement the FATF data, the evaluation utilizes additional measures and information relevant to judging a country's ability to prevent proliferation financing, such as estimates about the size of a country's black market or the extent of corruption.

Results

A central conclusion is that most countries do not perform well on preventing proliferation financing. In the ranking of this super criterion in 2017, no country achieved two-thirds of the available points and only two received more than half the available points. Many countries perform poorly due to having excessive bank secrecy, providing tax havens, and being places where front companies find it easier to finance nefarious activities. Other countries simply lack regulations and effective institutions.

Iran performs particularly poorly in the PPI, including on proliferation financing where it ranked at the bottom. Iran has been given extended time to fulfill its Action Plan requirements set out by the FATF and to comply with FATF standards. Recent actions have confirmed the deep

involvement of Iran's financial system in illicit activities. As a result, we recommend the re-imposition of FATF counter-measures against Iran.

The pie chart in figure 1 shows the fraction of countries that have scores exceeding 50 percent of the total, between 50 percent and 25 percent of the total, less than 25 percent down to a score of 0, and below a score of 0. Only two countries received more than half of the available points. About one-third of all countries achieved negative scores.

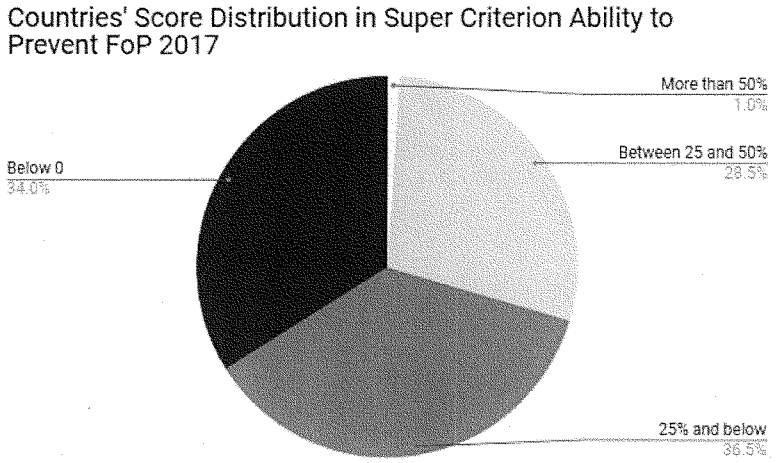

Figure 1. The pie chart shows the score distribution of countries in their *Ability to Prevent Proliferation Financing* in the PPI for 2017. The majority of countries score less than 25 percent of the available points. This figure includes corrected values for Viet Nam and Venezuela.

The PPI lists countries by score in the super criterion *Ability to Prevent Proliferation Financing,* which leads to a ranking. Although we do not release this ranking publicly, we provide below those countries that are in the top third and bottom ten percent by ranking.

Top third by rank (in alphabetical order):
Albania, Andorra, Antigua and Barbuda, Armenia, Australia, Austria, Bahamas, Bahrain, Barbados, Belgium, Bhutan, Botswana, Bulgaria, Burkina Faso, Cameroon, Canada, Chile, Cook Islands, Cyprus, Czech Republic, Denmark, Estonia, Fiji, Finland, France, Germany, Greece, Grenada, Hungary, Iceland, Ireland, Israel, Italy, Japan, Latvia, Lesotho, Liechtenstein, Lithuania, Macedonia, Malawi, Malta, Mauritius, Monaco, Nauru, Netherlands, New Zealand, Niue, Norway, Palau, Poland, Portugal, Romania, Samoa, San Marino, Singapore, Slovakia,

Slovenia, Solomon Islands, Spain, Sweden, Timor-Leste, Togo, Tonga, United Kingdom of Great Britain and Northern Ireland, United States of America, Uruguay, and Zambia.

Bottom 10% by rank (in alphabetical order):
Afghanistan, Belarus, Burundi, Democratic People's Republic of Korea (DPRK), Egypt, Eritrea, Iran (Islamic Republic of), Iraq, Lebanon, Libya, Morocco, Myanmar, Paraguay, Russian Federation, Serbia, Somalia, South Sudan, Sudan, Syrian Arab Republic, Thailand, and Ukraine.

Updates Since the Publication of the PPI 2017 regarding proliferation financing

Since the publication of the index, Institute staff have continuously updated and revised the data for a 2018 version of the ranking. Throughout the process, trends observed in the 2017 data on proliferation financing remain. Countries still perform poorly overall, and only three countries received 50 percent or more of the possible points.

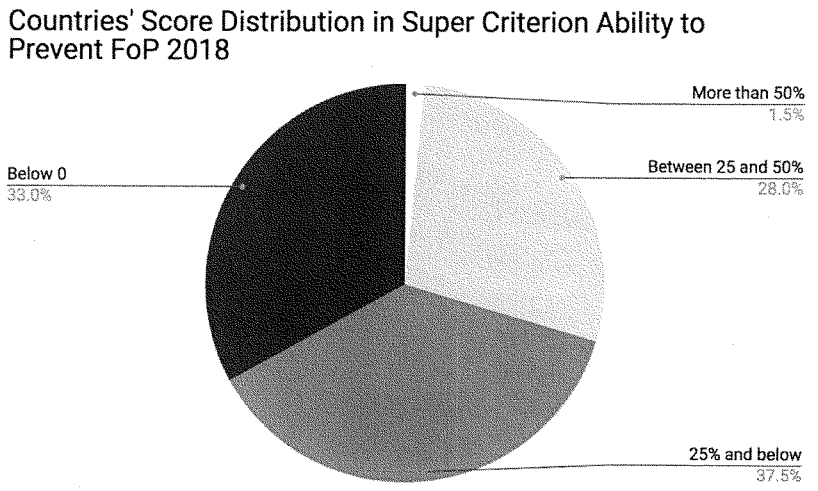

Figure 2. The pie chart shows the score distribution of countries in their *Ability to Prevent Proliferation Financing*, 2018 ranking. The majority of countries score less than 25 percent of the available points. In general, the distribution in these four broad categories has only minimally changed from 2017 and the need for further action is clearly visible.

As stated before, the PPI lists countries by score, generating a ranking. Although we do not release this ranking, we again provide those countries that are in the top third by ranking and the bottom ten percent in the 2018 ranking.

The top third of countries in the 2018 version are 80 percent the same as the 2017 version. 13 countries in the top third were replaced by other countries. For 2018, the top third countries are (alphabetically): Andorra, Angola, Antigua and Barbuda, Armenia, Australia, Austria, Bahrain, Bangladesh, Bhutan, Brazil, Bulgaria, Cameroon, Canada, Chile, Cook Islands, Croatia, Czech Republic, Estonia, Fiji, Finland, France, Germany, Grenada, Hungary, Iceland, Ireland, Israel, Italy, Japan, Latvia, Lesotho, Liechtenstein, Lithuania, Macedonia, Malawi, Malta, Mauritius, Mexico, Monaco, Mongolia, Nauru, Netherlands, New Zealand, Niue, Oman, Palau, Panama, Papua New Guinea, Poland, Portugal, Republic of Korea, Romania, San Marino, Saudi Arabia, Singapore, Slovakia, Slovenia, Solomon Islands, Spain, Sweden, Tonga, Trinidad and Tobago, United Kingdom of Great Britain and Northern Ireland, United States of America, Uruguay, Venezuela (Bolivarian Republic of), and Zambia.

The bottom 10 percent remained the same, except for three countries. For 2018, they are, alphabetically: Afghanistan, Belarus, Burundi, Central African Republic, DPRK, Egypt, Eritrea, Iran (Islamic Republic of), Iraq, Lao People's Democratic Republic, Lebanon, Libya, Morocco, Myanmar, Paraguay, Russian Federation, Serbia, Somalia, South Sudan, Sudan, and Tajikistan.

Comparison of Proliferation Financing Scores of PPI 2017 and PPI 2018

The point distribution graphs of countries' scores show that scores are generally increasing. Figures 3 and 4 show the point distribution graphs for 2017 and 2018, respectively. On average, all countries received two more points in the 2018 round of data collection than in the 2017 version.[4] Countries that received updates in FATF data, whether it be a new Mutual Evaluation Report or a new follow-up report, gained an average of six points based on that data alone. Since the end of the data collection period for 2017, the following countries received a new Mutual Evaluation Report: Andorra, Barbados, Botswana, Cambodia, Cuba, Denmark, Ethiopia, Ireland, Mexico, Mongolia, Nicaragua, Panama, Portugal, Slovenia, Thailand, and Ukraine. The following countries received a new follow-up report: Austria, Fiji, Hungary, Samoa, Suriname, Tunisia, and Vanuatu. Institute staff noted, however, that a new Mutual Evaluation Report did not always result in improvements and increased points. In some instances, countries' compliances were re-evaluated and given a "lower grade" than in a previous report.

The overall scores still cluster well below half the possible points (see figure 4). Ideally in the future, the cluster would move as a group toward higher points.

[4] The averages of points received are eight and ten in 2017 and 2018, respectively.

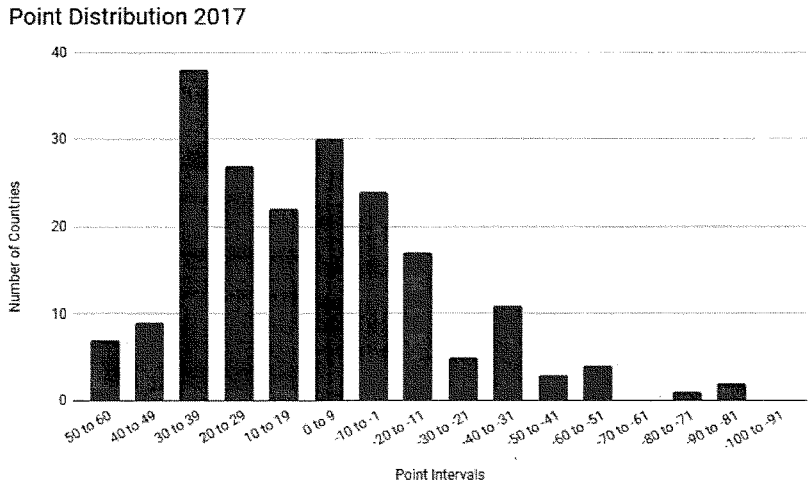

Figure 3. Point distribution based on data collected in 2017 out of a total of 110 points, excluding extra credit.

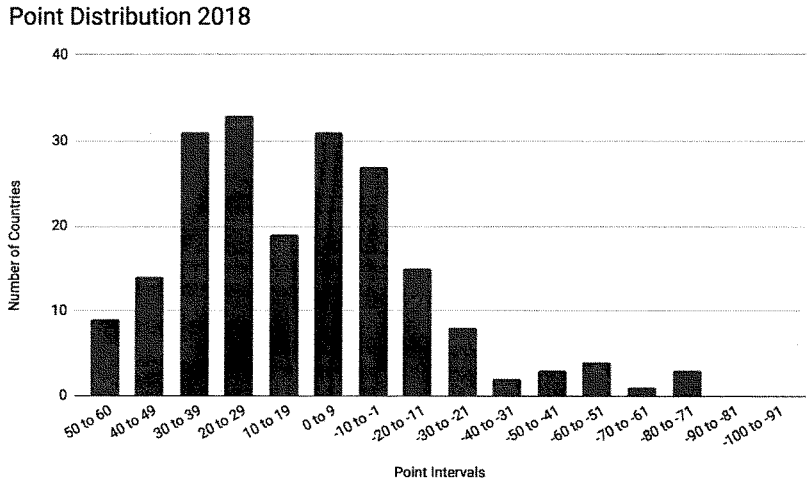

Figure 4. Point distribution based on revised data collected in 2018 out of a total of 110 points, excluding extra credit.

Summary of Key Findings and Recommendations:

In the Institute's PPI for 2017 ranking, the proliferation financing super criterion is the one in which countries collectively performed the worst. An overriding conclusion is that most countries do not perform well on preventing proliferation financing.

The Institute has developed a range of recommendations while producing the PPI and working with proliferation financing experts to develop its methodology. One of the most critical recommendations is that countering proliferation financing needs to be integrated into many more aspects of counterproliferation including export controls. Some specific recommendations follow.

1. All countries should work closely with FATF and its regional bodies to improve their efforts to prevent proliferation financing.
    1.1. They should also work to improve compliance with proliferation financing-relevant FATF recommendations.
    1.2. All countries should join or aspire to join FATF, if they have not already done so, and work closely with the organization to improve the integrity of their national financial controls against proliferation financing and other financial crimes. Israel is an example of a country that has prioritized joining FATF and is involved in a process of reviews. Membership and cooperation with FATF would not only reduce the chances that states' financial institutions will be used for the financing of proliferation, but also will reduce illicit outflows, the rise and permeability of black markets, and other nefarious business that could be taking place. Joining FATF is a way for countries to attract foreign investment and trade.
    1.3. Following coordination and assistance in bringing their controls into line with FATF-recognized best practices, countries should apply to have a mutual evaluation report conducted on them.

2. Each country should conduct a risk assessment of proliferation financing, and its agencies should address any gaps identified.
    2.1. Even though money laundering and terrorism financing may have similar indicators to proliferation financing, they should be differentiated from proliferation financing so that FoP risk assessments are comprehensive and accurate. Assessments should include expansive models of FoP rather than be based mainly on previous export and sanctions case studies.
    2.2. Each government should have adequate legislation in place; an effective system of coordination among departments working on FoP; well resourced, investigative Financial Intelligence Units; adequate enforcement; outreach to financial institutions; a system of mandatory sharing of information domestically (including sensitive information); ability to share information internationally; and

effective coordination with other governments.

3. A country's financial institutions need to be able to monitor, detect, report, and act upon suspicious financial transactions.
   3.1. Financial institutions need to have access to a secure and reliable mechanism to report suspicious financial transactions to the government. This includes the government creating adequate legislation mandating reporting, conducting outreach, and setting up points of contacts, as well as reporting mechanisms and ideally reporting requirements.
   3.2. Countries should help financial institutions identify and freeze suspicious transactions. Because of the difficulties of accomplishing this goal, the U.S. government should launch an interagency study to improve communication and information sharing with financial institutions, including insurance companies, and to develop better solutions for automated counter-proliferation financing screening tools.

4. Countries should participate in bilateral, multilateral, and law enforcement mechanisms to share FoP information and collaborate to enhance the effectiveness of counter proliferation financing efforts and facilitate adherence to international standards.
   4.1. Although there are many ways to implement this recommendation, one promising group for promoting cooperation among Financial Intelligence Units (FIUs) on FoP is the Egmont Group, which is a united body of 155 countries' Financial Intelligence Units.[5] The Egmont Group members' collaboration on money laundering and terrorism financing greatly improves the efficacies of the Financial Intelligence Units. The Egmont Group should expand its focus to specifically include proliferation financing. This could be accomplished through the inclusion of FoP criteria in the membership application and also through the development of an "Information Exchange on FoP Working Group."[6]

5. The Committee on United Nations Security Council Resolution 1540 (2004) should continue to promote the implementation of the financial control aspects of the resolution.
   5.1. The financing aspects of the 2017 matrix template mostly focus on terrorism financing. While item 11 in II. OP 2 - Nuclear Weapons (NW), Chemical Weapons (CW) and Biological Weapons (BW) refers to "Finance[ing] above mentioned activities,"[7] the matrices should be updated to more specifically

[5] "About - The Egmont Group," The Egmont Group, https://egmontgroup.org/en/content/about (Accessed July 9, 2018).
[6] The suggested name would be in line with the already existing "Information Exchange on ML/TF Working Group." See: "Information Exchange on ML/TF Working Group (IEWG)," The Egmont Group, https://egmontgroup.org/content/information-exchange-mltf-working-group-iewg (Accessed July 6, 2018).
[7] "Approved 1540 Committee Matrix (2017)," 1540 Committee, http://www.un.org/en/sc/1540/national-implementation/1540-matrices/matrix-template.shtml (Accessed July 9, 2018).

reference proliferation financing.

6. Efforts to prevent proliferation financing should be incorporated into export control regimes on a national basis and vice versa.
   6.1. National export control legislation should systematically include mechanisms and regulations to incorporate countering financial proliferation into governmental entities, including Financial Intelligence Units, in the processes of export control, including licensing decisions, enforcement, and customs clearance.
   6.2. Multilateral export control regimes should include FoP information in their deliberations and promote these efforts by adjusting their membership guidelines and sharing best practices to prevent proliferation financing.

7. FATF is in a unique position to drive many of the above-mentioned recommended actions and changes and should do so. Financing of proliferation should be treated broadly and as a separate subject to money laundering and terrorist financing.
   7.1. The FATF should add recommendations that more specifically focus on improving countries' capabilities to prevent and detect financing of proliferation. For example, it could integrate its 2008 "Indicators of Possible Proliferation Financing"[8] into recommendations, allowing them to evaluate countries' actions on preventing proliferation financing.
   7.2. At the plenary meetings, the FATF working group should discuss adjusting the language in several of the existing 40 FATF recommendations to extend them beyond CFT and AML, to include FoP. For example, FATF could encourage countries to conduct risk assessments for FoP by adding it to the language in Recommendation 1.[9]
   7.3. FATF should expand the number of categories it uses to evaluate countries with regard to proliferation financing and financial crime. For example, countries that actively improve their financial controls often remain in the partially compliant category, which may not encourage further improvements.
   7.4. FATF should standardize the evaluation process for all its regional bodies. It should seek to diminish disparities in levels of stringency utilized in the evaluations in order to bring about improved understanding of where countries stand in the FATF mutual evaluations and compliance categories.

8. Developed countries should encourage and provide resources to the FATF to increase the speed at which they conduct follow-up Mutual Evaluation Reports. This would reduce

[8] "Indicators of possible proliferation financing," as mentioned in Annex 1 to the 2008 FATF *Typologies Report on Proliferation Financing*. See: FATF, "Proliferation Financing Report," June 18, 2008, p. 54, http://www.fatf-gafi.org/media/fatf/documents/reports/Typologies%20Report%20on%20Proliferation%20Financing.pdf

[9] FATF Recommendation 1 is called "Assessing risks & applying a risk-based approach." For the full text of recommendations see: FATF, *International Standards on Combating Money Laundering and the Financing of Terrorism and Proliferation–The FATF Recommendations*, Paris, France, published February 2012, https://www.un.org/sc/ctc/wp-content/uploads/2016/10/fatf_recommendations_reprint2012.pdf

current lag times between countries self-reporting on their performance following a Mutual Evaluation Report, and FATF's verification process.

9. Fulfilling many of the PPI's sub-criteria under the *Ability to Prevent Proliferation Financing* super criterion, particularly improving a country's performance under many of the negative indicators, would strengthen financial controls overall.

10. Countries with advanced knowledge and experience in the area of countering proliferation financing should establish outreach programs that provide training and share best practices with countries seeking to improve financial controls.[10]
    10.1. In this effort, certain groups of countries should be prioritized and put under extra scrutiny and pressure. Such groups include responsible countries that nonetheless score particularly low in the PPI, those planning to acquire nuclear power reactors, and countries known to have violated financial sanctions on North Korea.[11]
    10.2. All UN member states should be encouraged to make use of a platform provided by the 1540 Committee, which helps to match countries seeking assistance with countries able to provide assistance.

Iran and FATF

Iran performs particularly poorly on the PPI and also does exceptionally poorly under the super criterion *Ability to Prevent Proliferation Financing*. It ranked 199 out of 200 in the ranking of this super criterion in 2017, and last overall for 2018.

Every year from at least 2008, Iran has been listed in the FATF annual public statements as a country with concerning anti-money laundering (AML) and counter-financing of terrorism (CFT) deficiencies. On February 25, 2009, FATF decided to publicly "call on its members and urge all jurisdictions to apply effective counter-measures to protect their financial sectors from money laundering and financing of terrorism risks emanating from Iran."[12] The only other country for which FATF had called such drastic measures was North Korea. Iran remained on the list of "high-risk and non-cooperative jurisdictions" for the subsequent seven years, until in June 2016, FATF suspended its countermeasures based on an Action Plan submitted by Iran. However, in February 2018, FATF stated that "Iran's action plan has now expired with a majority of the action items remaining incomplete."[13] It also stated, "Given that Iran has draft

[10] The PPI team was unable to locate many such programs outside of FATF.
[11] "How to Obtain the Book," Institute for Science and International Security, http://isis-online.org/ppi/detail/obtain-the-book/
[12] FATF, "FATF Public Statement - 16 February 2012," Paris, February 16, 2012, http://www.fatf-gafi.org/publications/high-riskandnon-cooperativejurisdictions/documents/fatfpublicstatement-16february2012.html
[13] FATF, "Monitoring Iran's actions to address deficiencies in its AML/CFT system," Outcomes of the FATF Plenary, February 21-23, 2018, Paris, February 23, 2018, http://www.fatf-gafi.org/countries/a-c/argentina/documents/outcomes-plenary-february-2018.html

legislation currently before Parliament, the FATF decided at its meeting this week to continue the suspension of counter-measures. Depending upon Iran's progress in completing its action plan, the FATF will take further steps in June 2018."

Civil society is not able to attend the FATF plenary meetings, but a Reuters report suggests that Iran was given extended time to fulfill its Action Plan requirements and that FATF will again address the issue in October.[14] Nevertheless, we assess that it is unlikely that Iran intends to fully implement its Action Plan and comply with FATF and the standards it sets in the future. In May 2018, the governor of the Central Bank of Iran was sanctioned by the U.S. Treasury's Office of Foreign Assets Control for assisting the Islamic Revolutionary Guard Corps' Quds Force with channeling money to Hezbollah. This shows how deeply involved Iran's financial system is in illicit activities.[15] On June 10, 2018, the Iranian parliament voted to suspend efforts to join the U.N. Convention for the Suppression of Financing of Terrorism, one of FATF's major requirements of Iran. On June 20, 2018, Iran's Supreme Leader Ayatollah Ali Khamenei, who is the ultimate decision maker on the country's policies, announced that he has no interest in joining the convention.[16] Therefore, we recommend the re-imposition of counter-measures against Iran.

[14] "Anti-money laundering body gives Iran until October to complete reforms," Reuters. June 29, 2018, https://www.reuters.com/article/us-iran-sanctions-fatf/anti-money-laundering-body-gives-iran-until-october-to-complete-reforms-idUSKBN1JP34N

[15] Toby Dershowitz, "Risks of Doing Business with Iran," *FDD Background Resource Guide* (Foundation for Defense of Democracies, Washington, D.C., June 21, 2018), http://www.defenddemocracy.org/media-hit/toby-dershowitz-risks-of-doing-business-with-iran1/

[16] Toby Dershowitz and Saeed Ghasseminejad, "Iran's supreme leader just torpedoed his country's best chance to get off the terror financing blacklist," *Business Insider,* June 22, 2018, http://www.businessinsider.com/iran-sank-its-best-chance-to-get-off-terror-financing-blacklist-2018-6

Appendix: Methodology used for the Super Criterion *Ability to Prevent Proliferation Financing* in the Peddling Peril Index for 2017

To develop a numerical ranking of performance on the super criterion *Ability to Prevent Proliferation Financing*, countries received points based on sub-criteria derived mostly from the FATF determinations. These sub-criteria assess countries' theoretical capabilities to prevent money laundering and proliferation financing based on their financial regulatory systems and counter-illicit financing programs. These eleven sub-criteria are characterized as "positive indicators."

The PPI then takes away points according to five "negative indicator" sub-criteria, or tangible information and examples of poor controls, such as when countries are known to have been involved in illicit finance, are sanctioned by major world economies for illicit financing activities, have assisted others in proliferation financing, or consistently do not act to prevent illicit financing efforts.

The positive and negative indicators are assigned a low, medium, or high impact for scoring purposes.

The project next assigns or takes away available "extra credit" points according to two other FATF-related sub-criteria. Finally, the judgment of experts in proliferation financing is used to take away or assign points based on their knowledge of proliferation financing in certain countries. After extra credit and expert knowledge points, a country could receive a total of 110 points for its *Ability to Prevent Proliferation Financing.*

Overall, there is little international effort devoted to assessing proliferation financing, which is why the PPI relies heavily on FATF evaluations. However, much of the FATF's information applies to broader illicit financing activities rather than specifically to proliferation financing. FATF only added proliferation financing as a focus in 2012. Since then, FATF evaluations include looking at countries' theoretical ability to implement international financial sanctions and the effectiveness of the controls against those countries under international financial sanctions, including investigation and enforcement actions. This evaluation data was only available for a limited number of countries. Thus, the PPI team decided to factor in the other point addition and subtraction categories.

Positive indicators:

- Compliance with selected FATF recommendations (for how recommendation 7 and Immediate Outcome 11 are evaluated, see below under Extra Credit)

  FATF is the organization that provides the most data regarding a country's banking

regulations and practices. The objectives of FATF are to set standards and promote 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 publishes a periodically updated set of recommendations that all member countries should follow to prevent financial crimes and publishes evaluations of individual counties' compliance with each recommendation. The evaluations are conducted by FATF or its regional FATF bodies and are titled *Mutual Evaluation Reports*. For each recommendation, potential deficiencies are listed, and a final conclusion is drawn, which can be that the country is Not Compliant, Partially Compliant, Largely Compliant, or Compliant with the specific recommendation. With the emergence of additional threats to the international financial system, including terrorist financing, and subsequently proliferation financing, FATF recognized the need to update its recommendations in 2003, and again in 2012. The Mutual Evaluation Reports based on the 2003 guidelines versus the 2012 guidelines often number their recommendations differently, and as a result the PPI lists a recommendation and its associated year, such as FATF Recommendation 2 (2012), meaning it is the one from the 2012 guidelines. As of April 2017, only 31 countries have undergone an evaluation based on the 2012 standards. (As of June 2018, 43 countries have undergone a FATF evaluation based on 2012 standards). To establish common ground between countries that have undergone a FATF evaluation before and after 2012, the PPI team only took into consideration recommendations found in both the new and old guidelines. The following FATF recommendations (FATF R.'s) have been carefully evaluated and selected by consulting financing of proliferation experts as most relevant to preventing proliferation financing, based on their experience with what governments need the most to prevent this illicit activity[17]:

- FATF Recommendation 2 (2012) 31 (2003) National Coordination[18]: "Countries should have national [anti-money laundering/counter-terrorist financing] policies [...]. Countries should ensure that [...] relevant competent authorities, at the policymaking and operational levels, have effective mechanisms in place which enable them to cooperate, and, where appropriate, coordinate domestically with each other concerning the development and implementation of policies and activities to combat money laundering, terrorist financing and the financing of proliferation of weapons of mass destruction." This is a high impact indicator.

[17] For the full text of recommendations see: FATF, *International Standards on Combating Money Laundering and the Financing of Terrorism and Proliferation - The FATF Recommendations*, Paris, France, published February 2012, updated October 2016, http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF_Recommendations.pdf

[18] This formulation reflects the fact that Recommendation 2 in 2012 standards is the equivalent of Recommendation 31 in 2003 standards.

- FATF Recommendation 40 (2012 and 2003) International Cooperation / Other Forms of Cooperation: "Countries should ensure that their competent authorities can rapidly, constructively, and effectively provide the widest range of international cooperation in relation to money laundering, associated predicate offences and terrorist financing." This is a high impact sub-criterion.

- FATF Recommendation 10 (2012) 5 (2003) Customer Due Diligence (CDD): "Financial institutions should be prohibited from keeping anonymous accounts or accounts in obviously fictitious names. [...] The principle that financial institutions should conduct CDD should be set out in law. [...] Financial institutions should be required to verify the identity of the customer and beneficial owner before or during the course of establishing a business relationship or conducting transactions for occasional customers." This is a medium impact indicator.

- FATF Recommendation 13 (2012) 7 (2003) Correspondent Banking: Financial institutions should collect additional information before conducting cross-border correspondent banking, and they "should be prohibited from entering into, or continuing, a correspondent banking relationship with shell banks." It is a medium impact sub-criterion.

- FATF Recommendation 26 (2012) 23 (2003) Regulation and Supervision: Financial institutions should be licensed, registered, regulated, and subject to monitoring. "[...] Countries should not approve the establishment, or continued operation, of shell banks." This is a medium impact sub-criterion.

- FATF Recommendation 30 (2012) 27 (2003) Law Enforcement Responsibilities: "Countries should ensure that designated law enforcement authorities have responsibility for money laundering and terrorist financing investigations [...]." This is a low impact indicator.

  The PPI assigned points (with a maximum score of 65 points) based on country compliance with this selected set of FATF recommendations that encapsulate critical elements or essential features of a system that prevents proliferation financing.

- Unavailability of Trade Financing

  As part of its 2014 *Global Enabling Trade Index,* The World Economic Forum measures how easily a business can finance trade at an affordable cost, based on conducted Executive Opinion Surveys. According to the World Economic Forum definition, the cost of financing trade includes trade credit insurance and trade credit, such as letters of

credit, bank acceptances, advanced payments, and open account arrangements. Countries are ranked out of 138, with 1 being the easiest country in which to obtain trade financing and 138 being the most difficult. For the PPI, this is used as a low impact indicator to assess how attractive a country is as an illicit finance hub. In other words, the unavailability of trade finance can be a small deterrent to proliferation financing.

The reasons for this include: 1) 80 percent of trade financing takes place through "open accounts," i.e. wire transfers. So, the unavailability of trade finance can render only 20 percent of all transactions in a country susceptible to illicit financing activities[19] ; 2) Trade financing applies mainly to countries at the origin and end point of transactions and not to countries in-between, limiting the opportunities for exploitation; and 3) State-sponsored proliferation networks are likely willing to dedicate more financial resources than profit-seeking businesses, which could make unavailability of trade financing a deterrent because of the additional time, documentation, and paper trail required. Developing countries often have an unavailability of trade financing, but surprisingly some small, developed countries such as Lithuania or Portugal, have an unavailability of trade financing as well. Greater availability of trade financing is seen in common trading hubs such as Hong Kong and Malaysia, but also in smaller, inconspicuous countries such as Malta, Oman, and Bahrain. It is a medium impact indicator.

- Low cumulative illicit financial outflows[20]

  This indicator measures illicit financial outflows from developing countries in 2013. Data is collected and published by Global Financial Integrity. According to the organization:

  Illicit outflow, measured in millions of U.S. dollars, is money illegally earned, transferred, and/or utilized. Some examples of illicit financial outflows listed might include:

  - *A drug cartel using trade-based money laundering techniques to mix legal money from the sale of used cars with illegal money from drug sales;*
  - *An importer using trade misinvoicing to evade customs duties, value added taxes (VAT), or income taxes;*
  - *A corrupt public official using an anonymous shell company to transfer dirty money to a bank account in the United States;*

[19] Jonathan Brewer, *Study of Typologies of Financing of WMD Proliferation, Interim Report* (London, United Kingdom: Project Alpha, King's College London, February 5, 2017), http://projectalpha.eu/wp-content/uploads/sites/21/2017/02/Study-of-Typologies-of-Financing-of-Proliferation-Interim-Report-5-Feb-2017.pdf

[20] Global Financial Integrity, *Illicit Financial Outflows from Developing Countries, 2004-2013*, See Appendix Table 5, Illicit Hot Money Narrow Outflows (HMN), May 1, 2017, http://www.gfintegrity.org/report/illicit-financial-flows-to-and-from-developing-countries-2005-2014/

- *A human trafficker carrying a briefcase of cash across the border and depositing it in a foreign bank; or*
- *A terrorist wiring money from the Middle East to an operative in Europe.*

As none of these are directly related to proliferation financing, the measure is deemed a medium impact indicator. Data are only collected for developing countries, which is useful as it balances out points that countries may have undeservedly received for having unavailable trade financing. Although illicit outflow is measured in absolute values, the PPI team took into account the size of illicit financial outflows in relation to a country's gross domestic product (GDP). Countries are awarded more points for not having large cumulative illicit outflows.

- Country has FATF or FATF Regional Body Membership[21]

FATF has established eight regional bodies to achieve global dissemination and coordination in order to promote better understanding and implementation of its international standards as highlighted in the FATF 40 (49 for post-2003) recommendations. Most countries are either FATF members or members of a FATF-style regional body; some are members of both. The level of organization and dynamic varies within the different groups. Before being able to become a FATF member, countries undergo a rigorous review process. FATF membership is awarded more points than regional body membership. The regional bodies are:

- The Eurasian Group (EAG)
- Asia/Pacific Group (APG)
- Caribbean Financial Action Task Force (CFATF)
- Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism of the Council of Europe (MONEYVAL)
- Eastern and Southern Africa Anti-Money Laundering Group (ESAAMLG)
- Financial Action Task Force on Latin America (GAFILAT)
- Intergovernmental Action Group Against Money Laundering in West Africa (GIABA).
- Middle East and North Africa Financial Action Task Force (MENAFATF)
- The Task Force on Money Laundering in Central Africa (GABAC)

This is a medium impact indicator.

[21] FATF, *Countries*, 2017, http://www.fatf-gafi.org/countries/

- FATF compliance score[22]

  The FATF compliance score is available for 90 countries on the 2015 *Financial Secrecy Index (FSI),* published by the Tax Justice Network. In the FSI, FATF compliance is indicator 11, "Anti-Money Laundering." According to the FSI report, compliance with all available recommendations (49 recommendations post-2003, or 40 recommendations post-2012) was calculated as a percentage, where "a 100% rating indicates that all recommendations have been rated as 'compliant', whereas a 0% rating indicates that the jurisdiction is wholly 'non-compliant.'"[23] Working with FATF to comply with general recommendations by implementing regulations and best practices is the first step for a country to prove its full commitment to financial transparency and anti-money laundering efforts. Despite some degree of duplication with the FATF recommendations above, this is a good indicator of general ability to prevent financial crimes. This is a medium impact indicator.

- Lack of denied parties by United States and European Union[24]

  Countries without entities sanctioned by the United States' OFAC, BIS, or the European Union's sanctions lists are viewed in general as having done better at detecting illicit activity and stopping it. Thus, for the PPI, these countries are viewed as capable of monitoring and detecting illicit activities and gain points. This sub-criterion allows for a rough measure of what a country knows about its internal business. Since it is only a rough measure, it is assigned low impact.

Variability in FATF compliance evaluations

In ranking the 31 countries that underwent the 2012 FATF evaluation, the PPI team noted that the way compliance judgments are made is not standardized throughout the regional FATF bodies. While some FATF bodies appear very strict and require that all deficiencies are removed before awarding a country the two highest levels of compliance (Largely Compliant and Compliant), other evaluating bodies seem to be more generous in assigning compliance levels. For example, the PPI team found that the European regional FATF body tends to be harsher in its

[22] Tax Justice Network, "Financial Secrecy Index - Country Reports," 2015, http://www.financialsecrecyindex.com/jurisdictions

[23] Tax Justice Network, "Key Financial Secrecy Indicators," July 22, 2015, http://www.financialsecrecyindex.com/PDF/11-Anti-Money-Laundering.pdf

[24] United States Department of the Treasury, Office of Foreign Assets Control, "SDN List by Country," https://www.treasury.gov/ofac/downloads/ctrylst.txt ; United States Department of Commerce, Bureau of Industry and Security, "Supplement No. 4 to Part 744 - ENTITY LIST," *Export Administration Regulations*, https://www.bis.doc.gov/index.php/forms-documents/regulations-docs/federal-register-notices/federal-register-2014/957-744-supp-4-1/file (Accessed Winter 2016); European Commission, "European Union - Restrictive measures (sanctions) in force," Updated April 26, 2017, https://eeas.europa.eu/sites/eeas/files/restrictive_measures-2017-04-26-clean.pdf. A change from last year is that the United States is not treated differently in regard to European Union sanctions.

assessments. The CFATF, or Caribbean regional body, and GAFILAT, or Latin American regional body, seem more generous in their assessments, which skews the outcome for a ranking.

Explanation for the need for additional negative indicators:

The final ranking would be less reliable if only the positive FATF-derived sub-criteria above were used to derive a ranking in this super criterion. Although FATF is the only organization that systematically tracks countries' actions to improve legal financial controls aimed at reducing threats to the integrity of the international financial system, its reporting contains many gaps. As discussed above, not all countries have been evaluated based on the 2012 standards, in particular FATF Recommendation 7 and Outcome 11, which directly relate to preventing proliferation finance. These gaps complicate gaining insights into what many countries do to prevent financial crime. The extent to which these gaps impacted the PPI ranking is difficult to evaluate.

Another issue concerns the FATF's evaluation methodology. Although the FATF evaluations are strong, there appear to be some potential weaknesses or biases that argue for the use of more sub-criteria. For example, compliance judgments published in follow-up FATF reports are derived based on a less rigorous evaluation process than the full reports. In follow-up reports, self-reporting plays a much greater role.[25] In addition, there are differences in how regional FATF organizations evaluate countries, as discussed above. This issue could risk that countries in certain FATF regions are ranked higher than what would be expected, based on other indicators such as money laundering. Lastly, FATF evaluations do not include the impact of enforcing UN financial sanctions on Iran and the DPRK. Those sanctions include a number of financial measures such as activity-based sanctions, vigilance requirements, and many others. Although these are described in non-binding FATF Guidance dated June 2013, they are not formally evaluated during the mutual evaluation processes. This issue could imply that countries may be doing better than the Mutual Evaluation Reports conclude.

A method was developed to more effectively rank countries under this super criterion because the number of positive sub-criteria based on FATF information has already relatively low and FATF information was not complete. This additional set of sub-criteria focus on negative outcomes, such as the existence of substantial black markets in countries or countries having a high number of sanctioned entities. A negative sub-criterion means that points are subtracted instead of added.

Negative indicators:

[25] See Organisation for Economic Co-operation and Development, Annex 2. A1, "A Note on FATF Data," in *Illicit Financial Flows from Developing Countries: Measuring OECD Responses*, 2014, https://www.oecd.org/corruption/Illicit_Financial_Flows_from_Developing_Countries.pdf

- Presence of denied parties by United States and European Union[26]

  Countries with entities sanctioned by the United States' OFAC, BIS, or the European Union's sanctions lists likely failed to detect illicit activity until after it occurred. Thus, for the PPI, these countries are treated as less capable of monitoring and detecting illicit activities. When assigning points for this sub-criterion, the number of entities was not taken into consideration, but more points were taken away for a country having entities on multiple sanctions lists. It is measured as a negative indicator with high impact, since it indicates actual instances where illicit activity has been detected.

- Appearance on the 2017 State Department List of Countries posing Money Laundering and Financial Crime concerns[27]

  The State Department Bureau for International Narcotics and Law Enforcement Affairs identifies in its March 2017 report "Countries/Jurisdictions of Primary Concern" for "Money Laundering and Financial Crimes." Using country profiles, the report points out weaknesses in those countries' enforcement or justice systems which pose challenges to the implementation of financing regulations. Examples of observed implementation challenges include "limited resources, lack of technical expertise, and poor infrastructure" as well as "administrative hurdles" and "corruption." This sub-criterion is medium impact.

- Worldwide Biggest Black Markets ranking[28]

  This indicator is a ranking of the world's 93 biggest black markets published by Havoscope, measured by their size in U.S. dollars. Although the size was measured in absolute values, the PPI team took into account the size of the black market in relation to a country's GDP. Black markets are linked to financial proliferation because they facilitate the financing of the illicit procurement of goods, which require secretive means. It is a medium impact sub-criterion.

---

[26] United States Department of the Treasury, Office of Foreign Assets Control, "SDN List by Country," https://www.treasury.gov/ofac/downloads/ctrylst.txt ; United States Department of Commerce, Bureau of Industry and Security, "Supplement No. 4 to Part 744 - ENTITY LIST," *Export Administration Regulations*, https://www.bis.doc.gov/index.php/forms-documents/regulations-docs/federal-register-notices/federal-register-2014/957-744-supp-4-1/file (Accessed Winter 2016); European Commission, "European Union - Restrictive measures (sanctions) in force," Updated April 26, 2017, https://eeas.europa.eu/sites/eeas/files/restrictive_measures-2017-04-26-clean.pdf

[27] United States Department of State, "International Narcotics Control Strategy Report - Money Laundering and Financial Crimes," Bureau for International Narcotics and Law Enforcement Affairs, Volume 2, March 2017, https://www.state.gov/documents/organization/268024.pdf

[28] Havocscope Global Black Market Information, "Havocscope Country Risk Ranking," http://www.havocscope.com/country-profile/ (Accessed July 2017).

- Significant illicit financial outflows[29]

  This indicator again uses data collected and published by Global Financial Integrity, measuring illicit financial outflows from developing countries in 2013. The PPI team decided that significant illicit financial outflows should be penalized. Points are taken off for countries that had more than $100 million in illicit financial outflows in 2013. It is a medium impact indicator.

- Lack of influence of corruption[30]

  Corruption can interfere significantly in the implementation of financial controls. Companies engaged in exporting may believe they can simply ignore any legal export or financial requirements if they believe there is little likelihood of being investigated or prosecuted. Corruption would likely inhibit strong financial controls and enforcement. In this sub-criterion, the 2016 Corruption Perceptions Index (CPI) by Transparency International is used as a measure of corruption in 176 countries. This index was selected from a variety of corruption measures and indices, mainly because this index lists the most countries and is widely respected. The PPI team used the rank of a country in the CPI to assign points, rather than its score derived by Transparency International. The points in this sub-criterion were assigned in an inversely proportional way to their relative rank. If the country or entity did not appear on the CPI, it was not assigned points. This sub-criterion has a medium impact.

"Extra-Credit" Opportunity:

For the 31 countries that were evaluated according to post-2012 FATF standards, the PPI offered an "extra credit opportunity," which allowed for the addition (or in a few cases the subtraction) of points. Information on those countries is included in the PPI scoring because the 2012 standards are of higher relevance than the previous sets of recommendations. For the first time, a recommendation specifically addresses a country's ability to implement targeted financial sanctions related to proliferation as laid out under relevant UN Security Council resolutions. Normally, if data were available for only about 30 countries, the PPI would not include this sub-criterion in the total. In this case, however, because of the direct relevance and importance of these post-2012 evaluations, the PPI adjusted its methodology to include the countries in a way that did not punish the other 170 countries. Therefore, the above-mentioned 31 countries were able to obtain extra points (or suffer subtractions) on top of the 110 total possible points if they

[29] Dev Kar and Joseph Spanjers, "Appendix Table 5: Illicit Hot Money Narrow Outflows (HMN)," in *Illicit Financial Flows from Developing Countries: 2004-2013* (Washington, D.C.: Global Financial Integrity, 2015), http://www.gfintegrity.org/report/illicit-financial-flows-from-developing-countries-2004-2013/. This sub-criterion was modified in the 2018 ranking.

[30] Those countries or entities not included in the CPI but evaluated by the PPI are: Andorra, Antigua and Barbuda, Belize, Cook Islands, Equatorial Guinea, Fiji, Holy See, Kiribati, Liechtenstein, Marshall Islands, Micronesia, Monaco, Nauru, Niue, Palau, Palestine, Saint Kitts and Nevis, Samoa, San Marino, Swaziland, Tonga, and Tuvalu.

were evaluated as largely compliant or compliant (or non-compliant) with the new UN financial sanctions-related recommendation.

Extra Credit indicators:

- Compliant or largely compliant with FATF Recommendation 7 (2012)[31]

  FATF recommendation 7 (2012) refers to implementation of targeted financial sanctions related to proliferation. It states, "Countries should implement targeted financial sanctions to comply with United Nations Security Council resolutions relating to the prevention, suppression and disruption of proliferation of weapons of mass destruction and its financing. These resolutions require countries to freeze without delay the funds or other assets of, and to ensure that no funds and other assets are made available, directly or indirectly, to or for the benefit of, any person or entity designated by, or under the authority of, the United Nations Security Council under Chapter VII of the Charter of the United Nations." A compliant or largely compliant score for R. 7 would allow a country to receive 10 additional points.

- FATF Immediate Outcome (IO) 11: Proliferation financial sanctions[32]

  Immediate Outcome 11 states, "Persons and entities involved in the proliferation of weapons of mass destruction are prevented from raising, moving and using funds, consistent with the relevant UNSCRs." As such, IO 11 also refers to implementation of targeted financial sanctions related to proliferation. It assesses whether persons and entities involved in the proliferation of WMD are prevented from raising, moving, and using funds consistent with the relevant UNSCRs. IO 11 is measured in terms of a low, moderate, or substantial level of effectiveness, where a country only received points for "substantial." Examples of outcomes evaluated by the FATF are concrete actions that have been taken, including investigations and prosecutions relating to sanctions. A substantial rating for IO 11 allows a country to gain five points.

Expert Judgment:

One final modification to the super criterion score resulted from extensive expert discussions. The PPI team considered the fact that there may be missing data relevant to the sub-criteria and experts often have the best, first-hand information about a country performing significantly

[31] FATF, *International Standards on Combating Money Laundering and the Financing of Terrorism and Proliferation - The FATF Recommendations*, Paris, France, published February 2012, Updated October 2016, http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF_Recommendations.pdf

[32] Financial Action Task Force, "An effective system to combat money laundering and terrorist financing," http://www.fatf-gafi.org/publications/mutualevaluations/documents/effectiveness.html (Accessed November 2017).

better or worse than scored. In some cases, experts judged that a country had received too many or too few points based on real-world knowledge and information.

Impact and Flow Chart of Sub-Criteria:

The PPI assigned a low to high impact for weighting each of the positive and negative sub-criteria. Table 5.1 found in the Peddling Peril Index for 2017, and reproduced at the end of the appendix, shows the flow chart of steps in the evaluation where positive indicators add points, negative indicators take away points, extra credit takes away or adds points, and expert judgment is factored in.

Other Criteria Considered

Institute staff considered additional sub-criteria but were unable to find enough information, so they were not included in the scoring. An example is the extent of training and knowledge of financial officials.

Ideally, the PPI team would measure if a country has access to, and participates in, training and outreach programs relating to proliferation finance. However, information on this topic proved difficult to find. There does not seem to be much international assistance offered to countries wanting to improve proliferation financing prevention. General bilateral trainings to prevent financial crimes are conducted by the United States Federal Reserve System, Department of Homeland Security, Department of Justice, Federal Bureau of Investigation, Department of State, and Department of Treasury. The U.S. State Department has organized regional conferences and specific outreach events for countering FoP training, such as in South Korea and Qatar (2013) and Vienna (2015). The Asia-Pacific Group has also actively holds workshops for its members.

Scoring:

The *Ability to Prevent Proliferation Financing* super criterion incorporates 11 positive sub-criteria, five negative sub-criteria, two extra credit, case-by-case sub-criteria, and finally expert judgment, where countries could receive or lose additional points. The positive and negative sub-criteria are evaluated in terms of low, medium, or high impact. Of the 11 positive sub-criteria, two are considered low impact, seven are medium impact, and two are high impact. They are worth 5, 10, and 15 points, respectively. Of the five negative sub-criteria, four are medium impact and one is high impact. Before extra credit and expert knowledge points, a country could receive a total of 110 points under this super criterion. Because of subtractions, negative scores are possible. This raw score is used later to arrive at a total, weighted score and rank for each country. It is also used to derive a ranking for the country.

Table 5.1. Impact and point adjustment for Super Criterion *Ability to Prevent Proliferation Financing.*

High Impact	Medium Impact	Low Impact
Positive indicators (points are added):		
FATF R. 2 (2012) 31 (2003) National Coordination	(Un)availability of trade finance	FATF R. 30 (2012) 27 (2003) Law Enforcement Responsibilities
FATF R. 40 (2012 and 2003) International Cooperation / Other Forms of Cooperation	FATF R. 10 (2012) 5 (2003) Customer Due Diligence	Lack of denied parties by US and EU
	FATF R. 13 (2012) 7 (2003) Correspondent Banking	
	FATF R. 26 (2012) 23 (2003) Regulation and Supervision	
	Low cumulative illicit financial outflows	
	FATF and Regional Body Membership	
	FATF Compliance Score	
⬇		
Negative indicators (points are subtracted):		
Presence of denied parties by US and EU	2017 State Department List of countries posing money laundering/financial crime concern	
	Worldwide Biggest Black Markets ranking	
	Significant illicit financial outflows	
	Lack of influence of corruption	
⬇		
Extra credit (points are added or subtracted on a case-by-case basis):		
Compliant or largely compliant with FATF R. 7 (2012) Substantial level in FATF Immediate Outcome 11		
⬇		
Expert judgment (points are added or subtracted on a case-by-case basis)		

RUSI
www.rusi.org

TESTIMONY BEFORE THE HOUSE COMMITTEE ON FINANCIAL SERVICES SUBCOMMITTEE ON TERRORISM AND ILLICIT FINANCE

Countering the Financial Networks of Weapons of Proliferation

Tom Keatinge, Director of the Centre for Financial Crime and Security Studies at the Royal United Services Institute

Introduction

Chairman Pearce, Ranking Member Perlmutter, and distinguished members of the Subcommittee, thank you for inviting me to testify today about strategies to disrupt the financing and procurement of weapons of mass destruction; and the role financial institutions (broadly defined) can play in identifying proliferation financing activities. Given my home base is London and the focus of RUSI's counter proliferation finance (CPF) research is on Southeast Asia and sub-Saharan Africa, my remarks will necessarily address to a greater extent the international CPF architecture, as promoted by bodies such as the United Nations and Financial Action Task Force (FATF), rather than the policies laid out by US domestic agencies. The US however, has a key role to play in strengthening this architecture, particularly as it takes on the Presidency of the FATF for the next 12 months.

Since 2015, thanks to the generous funding support of the John D and Catherine T MacArthur Foundation, RUSI has conducted extensive and wide-reaching research into the global counter-proliferation finance regime, assessing the awareness and effectiveness of governments and their private sectors in implementing proliferation finance controls.

Our research has produced four main papers as detailed below, all of which are freely available to governments and private sector actors:

- 2016: Out of Sight, Out of Mind? A Review of Efforts to Counter Proliferation Finance
- 2017: Countering Proliferation Finance: An Introductory Guide for Financial Institutions
- 2017: Countering Proliferation Finance: Implementation Guide and Model Law for Governments
- 2018: Underwriting Proliferation: Sanctions Evasion, Proliferation Finance and the Insurance Industry

We have also conducted outreach and training presentations in a number of countries in Southeast Asia, Europe and Africa, working closely with key government and private sector stakeholders in those countries to strengthen national responses to the illicit financial networks of proliferators. This work will continue in 2018/2019.

Consistent with the focus of the hearing, this submission, primarily based on the above-referenced titles published by RUSI, will cover the following fields: a background to the CPF status quo; a review of currently assessed global CPF capabilities; observations on and recommendations for the role of

financial institutions in tackling proliferation; wider supply chain vulnerabilities; and recommendations for stakeholder action.

Background

In 2012, the Financial Action Task Force (FATF), the international organisation responsible for co-ordinating government actions to counter financial crime and in which the US plays a leading role, broadened its recommendations to include measures relating to countering the financing of WMD, their delivery vehicles, and related goods and activities. The move to include this subject alongside terrorist financing and money laundering was seen by many of FATF's member states as a vital next step.

Prior to 2012, national efforts to combat proliferation finance had been highly uneven, and in many cases non-existent, despite UN Security Council resolutions, including Resolution 1540 and country-specific regimes, that detailed actions to counter proliferation finance. Although most countries had procedures in place to detect and prevent the flow of goods related to illicit WMD programmes, they did not have similar procedures in place to stem the flow of funds used to facilitate this dangerous trade.

Thus, independent, international leadership was needed to create a standard for CPF that would hinder the ability of proliferators to access and exploit the financial system. The FATF seemed ideally placed to offer such leadership.

When we began our research at RUSI, nearly four years had passed since the FATF incorporated recommendations on CPF into its international standards. Yet, despite the focus brought to the issue of proliferation finance by the FATF, RUSI's extensive interviews with governments, regulators and financial institutions (FIs) revealed that many of the shortcomings of the pre-2012 CPF landscape persisted. Put simply, very little had been done to put into effect the intentions expressed by the FATF in 2012 when it added CPF to its priorities. Governmental interest in proliferation finance and related outreach to FIs was highly uneven between national jurisdictions, with many countries providing no guidance on CPF to their financial sectors at all. The wide spectrum of approaches resulted in mixed messages being passed down from governments and regulators to their FIs.

For their part, FIs within FATF jurisdictions appeared generally alert to their obligations to enforce targeted financial sanctions (TFS) against individuals and entities specified in UN Security Council resolutions. Yet they were often ignorant of the enabling role of finance for proliferation networks and thus the proliferation threat beyond those sanctioned entities; they demonstrated a poor understanding of the nature of proliferation as an activity distinct from general sanctions evasion by states such as Iran and North Korea.

FIs were therefore often unclear as to what, if anything, they were expected to do to address the issue of proliferation finance beyond implementing TFS, believing in many cases that the CPF objective was achieved purely by avoiding business related to Iran and North Korea.

The combination of mixed messages, unclear expectations and lack of guidance meant that unsurprisingly FIs were struggling to devise their own internal approaches to mitigate relevant risks.

This has resulted in proliferators, such as North Korea, being able to access and abuse the international financial system in support of their proliferation ambitions with relative ease. The nuclear ambition of a state such as North Korea requires both the procurement of material and the raising of funds to source the required goods and services, and access to the international financial system is key to carrying out these activities. It thus seems axiomatic that targeting the financial networks of proliferators should be a global response to such threats.

To-date, the international community has primarily addressed state-based proliferation activity via controlling certain goods and sanctioning bad actors. Yet this approach is fragmented, poorly enforced and too narrowly focused. As a cursory review of the UN North Korea Panel reports will reveal, proliferators such as North Korea employ an array of funding operations, such as repairing and servicing military equipment; training police forces; and building statues, and a range of commercial trading activities which involve both a logistical and financial operation. All of these activities generate money flows.

Thus, focusing merely on goods, either preventing their sale or interdicting their transfer once purchased, is just one part of establishing an effective response. Proliferators depend on access to financial assets and services, and the international financial system has become a critical lifeline for the regime. Detecting and stopping financial access will complicate and obstruct the wider operations of proliferation networks.

Reviewing Current International Capabilities

The FATF is currently undertaking a global evaluation of countries' compliance with its 40 Recommendations for combatting financial crime, and the effectiveness of such compliance.

As of mid-May, 50 countries have been reviewed in the current round, running since 2014 (the US review was published in December 2016).[1]

Two primary elements of the FATF's review address CPF:

- Recommendation 7 assesses whether countries have the necessary frameworks in place to 'implement targeted financial sanctions to comply with United Nations Security Council resolutions relating to the prevention, suppression and disruption of proliferation of weapons of mass destruction and its financing' and that such frameworks should ensure that countries can 'freeze without delay the funds or other assets of, and to ensure that no funds and other assets are made available, directly or indirectly, to or for the benefit of, any

[1] United States, Mutual Evaluation Report (December 2016), available at http://www.fatf-gafi.org/countries/u-z/unitedstates/documents/mer-united-states-2016.html

person or entity designated by, or under the authority of, the United Nations Security Council under Chapter VII of the Charter of the United Nations.'[2]

- Immediate Outcome 11 characterises an effective system as one in which 'Persons and entities designated by the United Nations Security Council Resolutions (UNSCRs) on proliferation of weapons of mass destruction (WMD) are identified, deprived of resources, and prevented from raising, moving, and using funds or other assets for the financing of proliferation. Targeted financial sanctions are fully and properly implemented without delay; monitored for compliance and there is adequate co-operation and co-ordination between the relevant authorities to prevent sanctions from being evaded, and to develop and implement policies and activities to combat the financing of proliferation of WMD.'

Compliance with FATF Recommendations and Immediate Outcomes is assessed on a four-step scale from 'non-compliant' to 'compliant' and 'high' to 'low', respectively. The chart below, drawn from data provided by the FATF,[3] depicts the extent of assessed compliance and effectiveness for R7 and IO11 thus far.

	Recommendation 7 Compliance			Immediate Outcome 11 Effectiveness	
Compliant	8	16%	***High***	1	2%
Largely-	9	18%	***Substantial***	14	28%
Partially-	17	34%	***Moderate***	12	24%
Non-compliant	16	32%	***Low***	23	46%
Total	**50**	**100%**	**Total**	**50**	**100%**

USA rated Largely Compliant and High Effective in December 2016

As can be clearly seen, two-thirds of assessed countries are non- or only partially-compliant with the requirement to be able to impose TFS without delay; and 70% of assessed countries have a low or moderate level of effectiveness, meaning they suffer from major shortcomings.

It is clear that notwithstanding the prioritization of CPF in 2012, the global community still has considerable work to do to harden the financial system against abuse by proliferators.

It is important to note that compliance with FATF standards alone does not result in effective CPF controls. In fact, FATF's recommendations are now increasingly out of touch with other international obligations on CPF. UN sanctions against North Korea incorporate measures that go beyond list-based sanctions implementation, and focuses to a greater extent on activity-based obligations to counter proliferation finance. This includes requirements to restrict relationships with North Korean financial institutions and joint ventures. The recent FATF guidance published in March 2018 acknowledged this risk, stating that 'as list-based targeted financial sanctions alone cannot

[2] The FATF Recommendations, p11

[3] The Financial Action Task Force, *Consolidated Assessment Ratings* (18 May 2018), available at http://www.fatf-gafi.org/publications/mutualevaluations/documents/assessment-ratings.html

address illicit procurement and proliferation financing' implementation of UN measures that go beyond FATF requirements 'contributes to a stronger counter proliferation financing regime'.[4]

Furthermore, while the FATF requirement to implement targeted financial sanctions technically goes beyond those individuals and entities named on sanctions lists (to also include anyone owned by, controlled by or acting on behalf of or at the direction of those designated entities and individuals), this is not always reflected in implementation. It is RUSI's experience that countries and financial institutions focus on designated entities and individuals alone, and not their associated networks.

Securing the Financial System Against Abuse by Proliferators

Despite export control measures and international treaties seeking to prevent the further spread of nuclear, chemical and biological weapons and their related delivery systems, proliferators have been able to procure and acquire goods for these programmes with relative ease. International efforts to counter this have typically been devoted to the detection and seizure of physical goods, materials and technologies.

However, proliferation efforts rely also on finance to facilitate this illicit trade. Indeed, procurement of sensitive WMD-related goods is made possible by the international financial system. Reports from the UN Panel of Experts on North Korea, for example, have highlighted that Pyongyang is 'using greater ingenuity in accessing formal banking channels' to support illicit activities and WMD proliferation.[5] The most recent Panel report observes that North Korea 'continued to access the international financial system because of critical [sanctions] implementation deficiencies, which resulted in the country's evasive activities not being duly identified and prevented. The deceptive practices of the Democratic People's Republic of Korea and the lack of appropriate action by many Member States are systematically undermining the effectiveness of financial sanctions.'[6]

The role played by the financial sector in disrupting proliferation finance has received greater attention in recent years. Some governments maintain that financial institutions have both the capability to detect, and an obligation to disrupt, financial transactions in support of illicit WMD proliferation. However, government initiatives on countering proliferation finance vary widely between jurisdictions.

In addition to the research we have undertaken at RUSI to assess the capabilities of governments and their private sectors as relates to CPF, we also undertake training and provide technical assistance to these stakeholder groups -- particular FIs who are placed on the frontline of

[4] FATF, 'FATF Guidance on Counter Proliferation Financing', March 2018, p. 15.
[5] UN Security Council, 'Report of the Panel of Experts Established Pursuant to Resolution 1874 (2009)', S/2017/150, 27 February 2017, p. 4.
[6] UN Security Council, 'Report of the Panel of Experts Established Pursuant to Resolution 1874 (2009)', S/2018/171, 1 March 2018, p. 59.

implementation by their governments with limited support provided – to help equip them to better understand and mitigate proliferation financing risks.

This capacity-building activity reveals extensive gaps in knowledge, awareness and capabilities, and – perhaps more worryingly – highlights considerable misunderstanding with regards to the risks posed by proliferators, often conflating CPF activity with compliance with sanctions' regimes. We have found that while many FIs may have certain basic controls in place to counter proliferation finance, 'on the whole [they] do not understand the contemporary realities of the threat they are facing',[7] and are failing to implement adequate internal approaches to counter proliferation finance.

However, as outlined earlier, financial institutions have an important role to play in preventing proliferators from accessing the formal financial system and securing financial services in support of proliferation sensitive trade that goes beyond simply implementing targeted financial sanctions – as those on sanctions lists are unlikely to seek to transact in their own names.

It is therefore important that financial institutions take time to better understand and mitigate proliferation financing risk. Proliferators have become increasingly skilled at circumventing the sanctions imposed against them and gain access to the financial system through extensive networks of corporate entities (including front companies), middlemen and circuitous payment patterns.

In most cases, there will be no obvious paper connection to jurisdictions of proliferation concern. For financial institutions that have carried out little or no concerted thinking on this subject as distinct from other forms of financial crime, there are a number of approaches that can easily be adopted to improve the FIs contribution to CPF efforts. From our research at RUSI, we have identified three primary means by which the financial sector can support the hardening of the financial system against abuse by proliferators.

- First, situational awareness and education about the risk at hand: this includes conducting an internal risk assessment to better understand potential exposure to proliferation financing – as distinct from sanctions risk – and the areas of concern which would require mitigation. Few FIs interviewed by RUSI have made use of key information sources such as UN Panel reports and very few FIs identified a relevant staff member who tracked CPF associated publications from the FATF, UN or other government or academic bodies.

- Second, 'know your customer' (KYC) efforts should move beyond focusing merely on the entities and individuals listed on sanctions lists. Instead, FIs should familiarise themselves with the wider networks of proliferating actors. This includes ensuring that customer due diligence processes include the gathering of information that is relevant to proliferation financing, and not just other types of financial crime, and dedicating resources to conducting investigations into the networks of customers considered higher risk or operating in certain areas of the world, or sectors of the economy. While no approach to countering proliferation

[7] Emil Dall, Andrea Berger and Tom Keatinge., 'Out of Sight, Out of Mind? A Review of Efforts to Counter Proliferation Finance', RUSI Whitehall Report, 3-16 (June 2016), p. 19.

finance is fool-proof, a few simple adjustments to internal policies can go a long way to ensuring that a financial institution has a baseline policy for dealing with proliferation financing risk and can help mitigate the risk of inadvertently being caught up in proliferation financing activity.

- Third, identifying proliferation sensitive goods and technology: whilst the first two actions are relatively straightforward for FIs, identifying the procurement and shipping of proliferation sensitive goods is highly challenging, and arguably impossible for a financial institution to achieve, absent the provision of intelligence leads. Still, FIs should familiarise themselves with export control regimes, and which clients fall under those controls. FIs should also, having educated themselves about the risk of proliferation finance as part of the two previous actions, be aware of any transactions that fall outside of usual business activity and fit proliferation finance patterns.

Whilst there are clearly considerable improvements that FIs can make in staff awareness and fine-tuning KYC checks and due diligence processes to reflect proliferation finance risk, the CPF effectiveness of financial institutions will be greatly enhanced by information and intelligence support provided by national governments and international organisations. In our research, we found very few cases where governments worked with FIs to enhance their CPF capabilities, even if they had established partnership mechanisms for engaging with FIs on other issues such as terrorist financing and human trafficking.

Vulnerabilities Across the Supply Chain

The need for governments to engage with the private sector is not limited to a narrow definition of the financial sector. As sectoral sanctions have been increasingly applied to North Korea, it has undertaken creative and deceptive activity to secure funding from the sale of coal; it has also undertaken at sea ship-to-ship transfers to secure the energy products it needs. These activities bring into scope other industries needed to secure the integrity of the international supply chain that would benefit from engagement with national governments such as shipping companies, commodity brokers and insurance companies, all of which lag the banking sector in terms of awareness of, capability and commitment to the global CPF agenda.

Whilst the banking sector must continually strive to improve its standards, it is not right that it should be the only element of the private sector that invests in capabilities to address the deceptive practices of proliferators. A 'whole-of-system' approach is needed in order to maximise disruption opportunities.

Conclusions and Recommendations

As evidenced by the FATF's evaluation data and the detailed reports of the UN Panel of Experts on North Korea, six years since the FATF introduced CPF as a third leg of focus alongside money laundering and terrorist financing, global CPF efforts are fragmented at best and ineffective/non-existent at worst.

Furthermore, the current FATF standards related to CPF are weak and simplistic:

- They do not require countries to assess their proliferation financing risks
- They focus merely on the implementation of targeted financial sanctions
- They are not risk-based in their application

In sum, the global architecture for disrupting proliferation finance requires improved design and implementation.

The following recommendations are therefore offered for the Subcommittee's consideration.

For the private sector

- Financial institutions must expand their awareness of proliferators' activities and ensure that CPF is an integral part of their financial crime compliance and investigations capability, with designated expertise.
- Other related private sector actors such as insurance companies, commodity brokers and shipping companies need to demonstrate greater commitment to disrupting the ambitions of proliferators, in particular North Korea.
- The private sector as a whole needs to develop methods of collaboration that create a joined-up, whole-of-system response, that hardens the supply chain to abuse by proliferators.

For international organisations such as the FATF

- Although the FATF has recently made a welcome update to its CPF guidance,[8] with certain notable exceptions (such as the work undertaken by the FATF-style regional body in Asia, the Asia Pacific Group on Money Laundering), work across the FATF network on CPF lacks prioritisation. The country assessments conducted since 2014 highlight serious, systemic failings that need to be urgently addressed.

For the US Government

- From July 2018, the US assumes the presidency of the FATF (led by the Treasury Department's Office of Terrorist Financing and Financial Crimes). CPF is a stated priority of the US Presidency of the FATF over the next 12 months.[9] The US should use this position not only to continue efforts to raise global standards in line with current requirements, but also to review the adequacy of current FATF standards in order to promote opportunities to strengthen and broaden the status quo.
- Weaknesses in the global financial system will be exploited by bad actors, including proliferators and those seeking to raise funds in support of proliferation activities. A

[8] The Financial Action Task Force (2018), *Guidance on Counter Proliferation Financing – The Implementation of Financial Provisions of United Nations Security Council Resolutions to Counter the Proliferation of Weapons of Mass Destruction*, FATF, Paris www.fatf-gafi.org/publications/fatfrecommendations/documents/guidance-counter-proliferation-financing.html

[9] Outcomes FATF-MENAFATF Joint Plenary, 27-29 June 2018, available at http://www.fatf-gafi.org/publications/fatfgeneral/documents/outcomes-plenary-june-2018.html

continued, relentless focus on strengthening the integrity of the financial system, in its entirety, should be prioritised by the US Government.

For all national governments

- Financial institutions are placed on the frontline by the FATF, the UN and national governments. A failure by national governments to support the security role delegated to FIs results in material and systemic vulnerabilities. Establishing information exchange partnerships between governments and relevant private sector actors can greatly enhance the effectiveness of the role FIs are required to play.[10] The complexity of CPF for the private sector makes such partnerships critical to the development of an effective CPF response.

[10] For further details see Nick J Maxwell and David Artingstall (2017), The Role of Financial Information-Sharing Partnerships in the Disruption of Crime, RUSI Occasional Paper

Annex: Speaker and Organisation Details

Tom Keatinge, Director of the Centre for Financial Crime and Security Studies at the Royal United Services Institute

This submission is prepared by Tom Keatinge, the Director of the Centre for Financial Crime and Security Studies (CFCS) at the Royal United Services Institute (RUSI). RUSI is a donor-funded London-based defence and security think-tank, founded in 1831, and is registered with the Charity Commission for England and Wales (registration number: 210639).

Founded in December 2014, the CFCS is dedicated to addressing the challenges and effects of financial/economic crime and threat finance to the UK and international security and the important role finance can play in identifying and disrupting a range of globally-recognised threats. The team includes expertise from banking, law enforcement and international policy bodies such as the Financial Action Task Force.

Prior to joining RUSI in 2014, Tom was an investment banker with J.P. Morgan in London and New York for 20 years.

He has a Masters in Intelligence and International Security from King's College London, completed in 2012 whilst on a one-year sabbatical from J.P. Morgan. His Masters research focused on the effectiveness of the global counter-terror finance regime.

He has a BA in Modern Languages from the University of Durham (1990-1994).

CONGRESSIONAL TESTIMONY: FOUNDATION FOR DEFENSE OF DEMOCRACIES

House Financial Services Committee
Subcommittee on Terrorism and Illicit Finance

Countering the Financial Networks of Weapons Proliferation

DR. EMANUELE OTTOLENGHI

Senior Fellow
Foundation for Defense of Democracies

Washington, DC
July 12, 2018

Emanuele Ottolenghi July 12, 2018

INTRODUCTION

Chairman Pierce, Ranking Member Perlmutter, members of the subcommittee, on behalf of the Foundation for Defense of Democracies and its Center on Sanctions and Illicit Finance, I thank you for inviting me to testify.

The Islamic Republic of Iran has been under U.S. sanctions since late 1979. From 2006 to 2016, Iran's nuclear and ballistic missile programs were the target of a United Nations sanctions regime, which the United States, the European Union, and their Western allies (Australia, Canada, Japan, New Zealand, Norway, South Korea, and Switzerland) subsequently expanded with their own set of far-reaching measures. Initially designed to both punish and prevent proliferation attempts, these sanctions over time became wider in scope, eventually targeting Iran's energy industry, financial sector (including its Central Bank and most of its banking institutions), shipping, aviation, insurance, and oil exports.

Beginning in January 2016, the Joint Comprehensive Plan of Action, or JCPOA, granted Iran sanctions relief, though non-nuclear sanctions remained in force. Due to President Trump's May 2018 decision to withdraw from the JCPOA, Iran again faces U.S. sanctions, including secondary sanctions, which are already causing numerous international companies to withdraw from the Iranian market. Iran is therefore likely to ramp up its sanctions evasion efforts.[1]

Sanctions significantly inhibit Tehran's ability to trade with the world. Still, Iran has adapted, engaging sanctions enforcers in a complex and evolving cat-and-mouse game. With over three decades of experience eluding sanctions, Iran has displayed ingenuity and inventiveness to defy the embargo on its oil and petrochemical exports, bypass financial restrictions on its banking activities, and procure critical technology. Its responses to new sanctions have been quick and sophisticated. As a result, Iran has been able to mitigate sanctions' impact on its efforts to advance its nuclear and ballistic missile programs while keeping its economy afloat.

My testimony will outline how Iran evaded sanctions in the past, offering typologies as well as case studies in four areas of sanctions evasion: procurement, financial networks, fraudulent practices, and reliance on ancillary services.

PROCUREMENT

The simplest example of Iranian procurement is a triangular structure of front companies operating overseas. Iranian proxies usually establish fronts in a foreign country to procure dual-use technologies. Once incorporated, companies buy locally or from a third country. The buyer then ships the procured goods to the final destination in Iran, or fictitiously sells them to another front company in another country before final delivery.

A key factor in these schemes is the existence of an intermediate jurisdiction that obfuscates the merchandise's final destination. Over the years, the Iranian regime has established companies in Armenia, Azerbaijan, Georgia, India, Malaysia, Malta, Turkey, and the UAE for this purpose.

[1] See, for example: Storay Karimi, "Opportunities for Afghan money traders as sanctions loom," *Reuters*, June 30, 2018. (https://af.reuters.com/article/worldNews/idAFKBN1JR137)

Take, for example, the 2009 case of Majid Kakavand,[2] an Iranian citizen who established Evertop Services Sdn Bhd in the Malaysian capital of Kuala Lumpur to buy aerospace technology from Western suppliers for Iranian end-users.[3] Once the procured goods were delivered to Malaysia, Kakavand transferred them to Iran using an Iranian commercial cargo flight. Kakavand was arrested in France in March 2009 on charges of U.S. sanctions violations, though he successfully fought his extradition to the U.S.[4]

In a similar case, U.S. authorities accused Iranian national Hossein Tanideh of procuring technology on behalf of sanctioned Iranian nuclear procurement company MITEC,[5] through front companies he established in Turkey and Azerbaijan. Specifically, Tanideh sought to purchase valves for Arak's heavy water reactor from German manufacturers.[6] Locally based dual German-Iranian nationals facilitated the deal in Germany. When German officials grew suspicious, Tanideh turned to Indian manufacturers in his quest for a suitable alternative. Tanideh was added to OFAC's SDN list[7] and was sanctioned by the U.S. Department of State in July 2012 under Executive Order 13382 for proliferation.[8]

Such a scheme usually involves Iranian nationals opening companies abroad. But Tehran has also relied on Iranian expatriates who, as dual nationals, may raise less scrutiny, and foreign intermediaries, who act on their behalf. In a few cases, the intermediary works directly for the Iranian regime. More frequently, the proxy operates independently and works for a commission.

Mahan Air – an Iranian commercial airline under U.S. sanctions since 2011 – and its procurement efforts illustrate how a procurement scheme can adapt over time.[9] Initially, Mahan relied on overseas procurement companies to buy its planes and spare parts. These included Equipco UK

---

[2] David Albright, Paul Brannan, and Andrea Scheel Stricker, "Case Study - Middleman Majid Kakavand Arrested for Malaysia-Based Iranian Illicit Procurement Scheme," Institute for Science and International Security, February 26, 2010. (http://isis-online.org/isis-reports/detail/middleman-arrested-for-directing-malaysia-based-iranian-illicit-procurement/20)

[3] "Providing Additional Information to the Gos on Activities of the Swiss Firm Quartzcom (S)," *WikiLeaks Cable: 08STATE132055_a*, December 17, 2008. (http://cables.mrkva.eu/cable.php?id=183498); "Providing Belgium Additional Info on Malaysian Firm's Efforts to Purchase Data Acquisition Systems on Behalf of Iranian End-User (S)," *WikiLeaks Cable: 08STATE92637_a*, August 28, 2013. (https://www.wikileaks.org/plusd/cables/08STATE92637_a.html)

[4] Steve Erlanger and Nadim Audi, "France Won't Extradite Iranian Sought by U.S.," *The New York Times*, May 5, 2010. (http://www.nytimes.com/2010/05/06/world/europe/06france.html?_r=0)

[5] "Modern Industries Technique Company," *Iran Watch*, January 16, 2016. (http://www.iranwatch.org/iranian-entities/modern-industries-technique-company)

[6] Daniel Salisbury, "Illicit Procurement of German and Indian Valves for Iran's Arak Heavy Water Reactor," *Alpha*, June 20, 2013. (https://www.acsss.info/proliferation/item/242-mitec-s-procurement-of-valves-for-arak-heavy-water-reactor)

[7] U.S. Department of the Treasury, "Non-proliferation Designations; Non-proliferation Designation Removals; Iran Designations," July 12, 2012. (http://www.treasury.gov/resource-center/sanctions/OFAC-Enforcement/Pages/20120712.aspx)

[8] U.S. Department of State, "Increasing Sanctions Against Iran," July 12, 2012. (https://2009-2017.state.gov/r/pa/prs/ps/2012/07/194924.htm)

[9] U.S. Department of the Treasury, Press Release, "Treasury Designates Iranian Commercial Airline Linked to Iran's Support for Terrorism," October 12, 2011. (http://www.treasury.gov/press-center/press-releases/Pages/tg1322.aspx)

and Skyco UK in Great Britain, Kerman Aviation and Zarand Aviation in Paris, and Mahan Air General Trading and Sirjanco Trading in the United Arab Emirates – all run by Iranian nationals.[10] In the case of Turkey-based Pioneer Logistics, a Thai national who worked as a managing director for Mahan General Sales Agent in Bangkok appeared as a shareholder for the company, though he later admitted in a sworn affidavit that Mahan was the shares' real owner.[11]

When U.S. sanctions began to restrict Mahan Air procurement, Mahan again relied on proxies for its needs. Between 2006 and 2008, the airline sought the services of the British-based Balli Group to obtain Boeing aircraft. To conceal the end user for the planes, Mahan purchased the aircraft through UK-based subsidiaries and registered it with an Armenian subsidiary, Blue Airways.[12]

Using a similar scheme, in May 2015, Mahan took delivery of nine used Airbus aircraft[13] from Al-Naser Airlines, a small and privately owned Iraqi airline. Al-Naser bought eight planes from European companies and one smaller aircraft from a Chinese carrier, and then ferried them over to Iran after holding them in its custody for a short period. Treasury sanctioned Al-Naser shortly after the planes were delivered.[14]

More recently, Qeshm Fars Air, a carrier operating flights between Tehran and Damascus that are part of Iran's ongoing deliveries of military aid to Syria, procured two old Boeing 747 aircraft previously leased by a Georgian company and a now-defunct Armenian airline. The Iranian carrier began operating the aircraft in 2017.[15] Corporate records obtained by FDD suggest the aircraft owner was a Dubai-based company, at least until 2015, when the Armenian carrier took consignment of the aircraft.[16]

Such small triangular schemes are often temporary. Companies will typically shut down once they have accomplished their mission. For longer-term procurement and finance operations, Iran relies more on permanent corporate structures. Indeed, before sanctions forced Iran's procurement operations to go underground, large Iranian state companies had their own senior managers run their official procurement offices overseas. Some were eventually sanctioned, while others escaped designation even when their parent companies in Iran did not.[17]

---

[10] U.S. Department of Commerce, Press Release, "BIS Adds Three Parties to Temporary Denial Order Against Iranian Airline," April 17, 2012. (http://www.bis.doc.gov/index.php/component/content/article/98-about-bis/newsroom/press-releases/press-releases-2012/335-bis-adds-three-parties-to-temporary-denial-order-against-iranian-airline)

[11] U.S. Department of Commerce, Bureau of Industry and Security (BIS), "Order Renewing Order Temporarily Denying Export Privileges," June 21, 2018. (https://www.federalregister.gov/documents/2018/06/21/2018-13289/order-renewing-order-temporarily-denying-export-privileges)

[12] Laura Rozen, "UK firm pleads guilty to selling U.S. 747 to Iran," *Politico*, February 5, 2010. (https://www.politico.com/blogs/laurarozen/0210/UK_firm_pleads_guilty_to_selling_US_747s_to_Iran.html)

[13] Eli Lake, "With Plane Delivery, Sanctions Collapsing Already," *Bloomberg*, May 11, 2015. (http://www.bloombergview.com/articles/2015-05-11/with-plane-delivery-iran-sanctions-collapsing-already)

[14] U.S. Department of the Treasury, Press Release, "Treasury Department Targets Those Involved in Iranian Scheme to Purchase Airplanes," May 21, 2015. (http://www.treasury.gov/press-center/press-releases/Pages/jl10061.aspx)

[15] "Iran's Qeshm Fars Air begins B747 freighter ops," *Ch-Aviation*, April 1, 2017. (accessed via Ch-Aviation)

[16] "Aircraft Details – EP-FAA" *Ch-Aviation*, updated February 28, 2018, accessed July 5, 2018. (accessed via Ch-Aviation)

[17] For example, NIITCO GmbH, in Hamburg, Germany and its London subsidiary NIITCO (http://www.niitco.co.uk/contact.htm) belong to the Iranian Mines and Mining Industries Development and Renovation Organization (IMIDRO), a, Iranian government entity delisted by the JCPOA and therefore under U.S.

Iran has responded to sanctions by creating complex corporate structures across different jurisdictions, making the link with an Iranian parent entity less obvious. Iranian senior corporate managers often fictitiously resigned their government jobs to seek business ventures overseas on behalf of the regime, quickly emerging as proprietors of business empires with no formal ties with Iran. A regime proxy with no formal connection to past employers provides plausible deniability.

Former regime procurement agents interviewed by FDD confirm that Iranian state companies have increasingly entrusted their most capable senior management with significant sums to invest industrial assets abroad.[18] Ownership of Western factories gives Iran access to knowledge and technology. This was the case of MCS International GmbH – a gas cylinder factory in Germany formerly known as Mannesmann Cylinder Systems GmbH. Iranian interest in the factory derived from a dual-use flow-forming machine that MCS's production line used for carbon fiber and chromium molybdenum steel mixed products. Such machines are critical in the production of uranium enrichment centrifuges.

The story of how Tehran gained access to such sensitive dual use technology begins in 2003, when a group of Iranian investors purchased Mannesman Cylinder Systems in Dinslaken, Germany and renamed it MCS International GmbH. The company changed its name again in 2011 to MCS Technologies GmbH, and after a bankruptcy procedure, it was liquidated in April 2013. Corporate records show that from 2003 to 2011, MCS was owned by Reyco GmbH, a German subsidiary of Rey Investment Co. According to Treasury, Rey Investment Company was:

> ... formerly run by Ayatollah Mohammad Mohammadi Reyshahri, who previously served as the Iranian Minister of Intelligence and Security. Rey Investment Company collected and invested donations obtained from Iranian Shi'a shrines. However, amidst allegations of mismanagement and embezzlement of shrine donations from the company, the Iranian Government cut off its funding to the point of nearly bankrupting the company. In mid-to-late 2010, Reyshahri was removed and control of Rey Investment Company was transferred to EIKO [a conglomerate owned by the Supreme Leader of Iran] and its director. EIKO subsequently appointed a new Managing Director of Rey Investment Company.[19]

Rey Investment's mismanagement undermined the performance of its overseas holdings, including, critically, MCS International. But in 2011, Iranian assets in Europe operated under a new, more difficult business climate. The UN Security Council had passed four resolutions imposing sanctions against Iran's financial, commercial, and transportation sectors. The European Union had adopted expansive sanctions against the same sectors, as well as Iran's energy industry. The U.S. sanctions regime also included new executive and legislative measures. Rather than closing the factory and looking for new investments, Iran salvaged its German asset, obfuscating its ownership in the process. According to the June 4, 2013 Treasury designation:

---

sanctions since the U.S. stopped enforcing the JCPOA. Evidence obtained from the German and British commercial registries.

[18] Michael Birnbaum and Joby Warrick, "A mysterious Iranian-run factory in Germany," *The Washington Post*, April 17, 2013. (http://www.washingtonpost.com/world/europe/a-mysterious-iranian-run-factory-in-germany/2013/04/15/92259d7a-a29f-11e2-82bc-511538ae90a4_story.html)

[19] U.S. Department of the Treasury, Press Release, "Treasury Targets Assets of Iranian Leadership," April 4, 2013. (https://www.treasury.gov/press-center/press-releases/Pages/jl1968.aspx)

> MCS International was audited by [an EIKO subsidiary] in October 2010 and determined to be in poor financial standing. However, EIKO management rescued MCS International from bankruptcy and insisted on keeping the company open because it viewed MCS International as key to facilitating business in Europe. EIKO management viewed MCS International as being too important to EIKO's international plans to allow it to go bankrupt and believed that it would be easier to rescue MCS International from bankruptcy than to create or acquire new foreign companies on behalf of EIKO due to U.S. and international sanctions. EIKO subsequently ordered that responsibility for MCS International be transferred from EIKO-controlled TEACO to Iranian businessmen, who were sent to oversee the company. Following this transfer, the two individuals owned the shares for MCS International, but answered directly to EIKO.[20]

Commercial registry entries for MCS Technologies GmbH (aka MCS International) show that both registered owners were Iranian-Canadian dual nationals and Canadian residents.

Berichtigte Liste der Gesellschafter der Kronen tausend674 GmbH, Berlin künftig: MCS Systems GmbH, Dinslaken, gemäß § 40 Abs. 2 GmbHG

Nr.	Gesellschafter	Wohnort	Anteil mit Nr.
1	Abdolrasoul Dorri-Esfahani (geb. 04.04.1945) No. 130 b, Belsize Drive, Toronto, Ontario	No. 130 b, Belsize Drive, Toronto, Ontario M4S 1L8, Kanada	1 - 12.750 über je EUR 1,00
2	Eshagh Hajizadeh (geb. 03.11.1967)	1189 Shavington Street, North Vancouver, BC, V7LILI, Kandada	12.751 - 25.000,00 über je EUR 1,00

Commercial Extract for MCS Technologies GmbH showing two owners as residents of Canada

Though unable to move the equipment to Iran because of tough U.S. and EU sanctions, the regime's proxies controlled the asset for 10 years and arranged for periodic visits by engineering delegations from Iran. Iranian engineers spent time familiarizing themselves with MCS technology used for the production of uranium enrichment centrifuges. Eventually, Rey Foundation established a replica of MCS (Pars MCS) in Iran.[21]

Another prominent example of a former Iranian official entrusted with significant assets and latitude to assist the regime's sanctions evasion schemes is Mehdi Shamszadeh, the former

[20] U.S. Department of the Treasury, Press Release, "Treasury Targets Assets of Iranian Leadership," April 4, 2013. (https://www.treasury.gov/press-center/press-releases/Pages/jl1968.aspx)
[21] "Home: Pars Mcs," *Pars Mcs Website*, accessed June 22, 2015. (http://www.parsmcs.com/contents/index/lang/en)

commercial director for the Islamic Republic of Iran's Shipping Lines (IRISL).[22] Treasury sanctioned IRISL in 2008 for facilitating "shipments of military-related cargo destined for [Iran's Ministry of Defense Armed Forces and Logistics] and its subordinate entities, including organizations that have been designated by the United States pursuant to E.O. 13382 and listed by United Nations Security Council Resolutions 1737 and 1747."[23]

Shamszadeh moved to London in 2005 to serve as the local director of IRISL UK, a subsidiary of IRISL, and of IRINVESTSHIP Ltd, a financial holding company co-owned by IRISL. Treasury eventually sanctioned both in September 2008.[24] Shamszadeh, however, resigned both positions, launched his own businesses, acquired British nationality, and shortened his name to Shams.[25] He was never sanctioned, but Iranian authorities arrested him in 2015 upon entry into Iran and tried him for embezzling government money he acquired in the course of running a complex sanctions evasion scheme. Shamszadeh, who boasted of his contribution to the sanctions evasion effort during the trial proceedings,[26] was sentenced to death in early 2016. He appealed and his case is pending.[27]

FINANCIAL EVASION

Iranian officials in 2011 admitted that sanctions on its banking sector were painful.[28] UN sanctions only listed a handful of Iranian banks. U.S. and EU sanctions added more banks to the list, including Iran's Central Bank, and targeted Iranian banking subsidiaries overseas. From 2012 to 2016, Iranian banks were also removed from SWIFT, the Belgian-based cooperative clearing platform for international banking transactions.[29] With U.S. financial sanctions now re-imposed, Iranian banks will likely, once again, be cut off from the international financial system.

Iran's evasion of financial sanctions follows the same playbook as commercial restrictions. The regime first established and then sought to purchase banks outside Iran to facilitate prohibited banking transactions, adding successive layers of obfuscation to cover its tracks. Over the years, large Iranian banks have incorporated subsidiaries overseas: Arian Bank in Afghanistan,[30] Bank

---

[22] Cynthia Busuttil, "Iranian firm denies 'pressure' claims," *Times of Malta*, June 4, 2004. (http://www.timesofmalta.com/articles/view/20040604/local/iranian-firm-denies-pressure-claims.121313)
[23] U.S. Department of the Treasury, Press Release, "Major Iranian Shipping Company Designated for Proliferation Activity," September 10, 2008. (https://www.treasury.gov/press-center/press-releases/Pages/hp1130.aspx)
[24] U.S. Department of the Treasury, Press Release, "Major Iranian Shipping Company Designated for Proliferation Activity," September 10, 2008. (https://www.treasury.gov/press-center/press-releases/Pages/hp1130.aspx)
[25] "Directors' Particulars of Change," *Company House*, Corporate entry for Global Holding Investments Ltd., July 16, 2011.
[26] Tom Coghlan and Sean O'Neill, "Britain pleads for life of confessed sanctions buster," *The Times* (UK), April 11, 2016. (https://www.thetimes.co.uk/article/britain-pleads-for-life-of-confessed-sanctions-buster-n0ddjtcwg)
[27] Michael O'Kane, "Mehdi Shams sentenced with Babak Zanjani for Iran sanctions evasion," *European Sanctions*, April 13, 2016. (https://europeansanctions.com/2016/04/13/mehdi-shams-sentenced-with-babak-zanjani-for-iran-sanctions-evasion/)
[28] Rick Gladstone, "Iran Admits Western Sanctions Are Inflicting Damage," *The New York Times*, December 20, 2011. (http://www.nytimes.com/2011/12/20/world/middleeast/iran-admits-western-sanctions-are-inflicting-damage.html?_r=0)
[29] "Payments system SWIFT to expel Iranian banks Saturday," *Reuters*, March 15, 2012. (http://www.reuters.com/article/2012/03/15/us-nuclear-iran-idUSBRE82E15M20120315)
[30] "Arian Bank," *Iran Watch*, January 16, 2016. (http://www.iranwatch.org/iranian-entities/arian-bank)

Melli ZAO in Russia,[31] Future Bank in Bahrain,[32] Mellat Bank SB CJSC in Armenia,[33] Oner Bank ZAO in Belarus,[34] Persia International Bank PLC in Great Britain,[35] and Trade Capital Bank in Belarus.[36]

Iran also sought to facilitate Iranian financial activities by creating joint banking ventures in friendly jurisdictions.[37] Iranian banks established the European-Iranian Commercial Bank (EIH)[38] in Hamburg, Germany. In Venezuela, Iran created the Iran-Venezuelan Binational Bank[39] as a joint venture between the Export Development Bank of Iran and the Banco Industrial de Venezuela.

Once these were sanctioned,[40] Iranian strategy shifted from trying to establish banking institutions abroad to taking control of foreign banks. Iranian proxies did so at least twice.

In 2008, three Iranian businessmen, whom the U.S. Department of Treasury later sanctioned for acting on behalf of Iran, purchased a controlling stake in a small bank in Tbilisi, Georgia. The three incorporated a foundation in Liechtenstein, KSN Foundation, for the purpose of controlling Invest Bank JSC, as well as funds in Switzerland and New Zealand.[41] A December 2016 sanctions evasion case against a U.S.-Korean dual national acting on Iran's behalf revealed that the same three Iranians helped launder as much as $1 billion and more than €1 billion in oil revenues through their network.[42]

---

[31] "Bank Melli Iran Zao," *Iran Watch*, January 16, 2016. (http://www.iranwatch.org/iranian-entities/bank-melli-iran-zao)
[32] "Future Bank," *Iran Watch*, January 16, 2016. (http://www.iranwatch.org/iranian-entities/future-bank)
[33] "Mellat Bank SB CJSC," *Iran Watch*, January 16, 2016. (http://www.iranwatch.org/iranian-entities/mellat-bank-sb-cjsc)
[34] "Onerbank Zao," *Iran Watch*, January 16, 2016. (http://www.iranwatch.org/iranian-entities/onerbank-zao)
[35] "Persia International Bank PLC," *Iran Watch*, January 16, 2016. (http://www.iranwatch.org/iranian-entities/persia-international-bank-plc)
[36] "Trade Capital Bank," *Iran Watch*, January 16, 2016. (http://www.iranwatch.org/iranian-entities/trade-capital-bank)
[37] Douglas Farah, "Iran Moving Banking Operations to Latin America," *Douglas Farah Blog*, May 30, 2008. (http://blog.douglasfarah.com/article/356/iran-moving-banking-operations-to-venezuela.com)
[38] "Europaisch-Iranische Handelsbank AG," *Iran Watch*, January 16, 2016. (http://www.iranwatch.org/iranian-entities/europaisch-iranische-handelsbank-ag)
[39] "Inaugurado Banco Binacional Iran-Venezuela," *Partido Socialista Unido de Venezuela*, April 3, 2009. (http://www.psuv.org.ve/temas/noticias/Inaugurado-banco-binacional-Iran-Venezuela/)
[40] The U.S. Department of the Treasury targeted EIH in September 2010: U.S. Department of the Treasury, Press Release, "Treasury Department Targets Iranian-Owned Bank in Germany Facilitating Iran's Proliferation Activities," September 7, 2010. (http://www.treasury.gov/press-center/press-releases/Pages/tg847.aspx); The European Union followed suit in May 2011: Council Implementing Regulation (EU) No 503/2011 of 23 May 2011 Implementing Regulation (EU) No 961/2010 On Restrictive Measures Against Iran, *Official Journal of the European Union*, May 23, 2011. (http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2011:136:0026:0044:EN:PDF); The U.S. Treasury sanctioned the Iran-Venezuela Binational Bank in May 2013: U.S. Department of the Treasury, Press Release, "Treasury Targets Iranian Attempts to Evade Sanctions," May 9, 2013. (http://www.treasury.gov/press-center/press-releases/Pages/jl1933.aspx)
[41] Benoit Faucon, Jay Solomon, and Farnaz Fassihi, "As Sanctions Bite, Iranians Invest Big in Georgia," *The Wall Street Journal*, June 20, 2013. (http://www.wsj.com/articles/SB10001424127887323864304578320754133982778)
[42] *United States of America vs. Real Property Located at 11621 Alderwood Loop, Anchorage, Alaska et al*, 3:14-cv-00065 (D. Alaska April 7, 2014), page 20. (accessed via PACER)

Control over Invest Bank was wrested from Iranian hands in June 2013. The U.S. Treasury subsequently sanctioned KSN and the Iranian proxies involved,[43] though they were all delisted in January 2016 pursuant to the JCPOA. Evidence suggests[44] that their Georgia-based network is fully reconstituted to include a money exchange business, a financial assets management company, a stake in a new bank, and other assets.

Iran has also evaded sanctions by moving its assets to foreign accounts. The simplest destination for such funds is overseas subsidiaries of Iranian companies not yet sanctioned. These entities bank locally. They also transact locally with business counterparts, purchasing merchandise that transits through the countries where the subsidiaries are incorporated. With all business conducted locally, usually no red flags are raised.

A good example of this mechanism is Mapna Group's overseas operations. Mapna[45] is one of the largest Iranian energy sector service companies, with high profile public projects both in Iran and abroad. Iran's supreme leader gave his 2014 "resistance economy" speech, extolling the virtues of enduring sanctions and engaging in sanctions evasion, from Mapna's headquarters.[46] Mapna has been repeatedly denied export licenses by the British government for WMD proliferation concerns.[47]

The company holds great importance for the Iranian regime. Mapna's current chairman, Abbas Aliabadi, was a faculty member and the deputy manager of Emam Hossein University – the defense college of Iran's Islamic Revolutionary Guard Corps (IRGC). Mousa Refan, the founder of the IRGC air force, previously sat on the company's board of directors. Mapna belongs to the Reza Shrine Foundation (*Astane Ghods Razavi*),[48] whose chairman, Ayatollah Ebrahim Raisi, was directly appointed by, and reports to, the supreme leader.

Despite its close connections to the regime and its possible past role in WMD procurement, Mapna was never designated by the EU, UN, or U.S. However, its 33 subsidiaries in Iran, like every other Iranian business, suffered (and are likely to suffer again) from financial sanctions against Iran's banking sector.

To service its financial transactions, Mapna built a network of overseas subsidiaries and companies. These include: Mapna International FZE in Dubai; Mapna Europe GmbH in Germany;

---

[43] U.S. Department of the Treasury, Press Release, "Treasury Targets Networks Linked to Iran," February 6, 2014. (http://www.treasury.gov/press-center/press-releases/Pages/jl2287.aspx)

[44] Emanuele Ottolenghi, "Snap-Back: A journey through Iranian sanctions evasion in Georgia," *Tablet Magazine*, July 1, 2015. (https://www.tabletmag.com/jewish-news-and-politics/191903/iranian-sanctions-evasion)

[45] "Fields of Activity," *MAPNA Group Website*, accessed June 22, 2015. (http://www.mapnagroup.com/)

[46] Grand Ayatollah Sayyid Ali Khamenei, "Supreme Leader's Speech in Meeting With Laborers of MAPNA Group," *The Center for Preserving and Publishing the Works of Grand Ayatollah Sayyid Ali Khamenei*, April 30, 2014. (http://english.khamenei.ir//index.php?option=com_content&task=view&id=1903&Itemid=4)

[47] UK Department for Business Innovation & Skills, "Iran List (Last Amended 5 October 2015)," October 5, 2015. (https://web.archive.org/web/20160409060415/https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/466147/iran-list-oct-15.pdf)

[48] "پرتال جامع آستان قدس رضوی," *Astan Quds Razavi* (Iran), accessed June 22, 2015. (http://www.aqr.ir/Portal/Home/Default.aspx)

Mapna Italia SRL in Italy; Mapna International Shanghai in China; Qarn Muscat LLC in Oman; MS Uluslararasi Enerji Yatirim Anonim Şirketi, Özgüneş Elektrik Parçaları Ticaret Limited Şirketi, and Energy Trading Elektrik Sanayi Ve Ticaret Limited Şirketi in Turkey; and Kura Industrial Trading LLC in Tbilisi, Georgia. Corporate documents filed by some of these companies show that they lend each other funds. Documents leaked to FDD demonstrate that as of December 2011, both Mapna Europe GmbH and Mapna International FZE held an account at the Frankfurt branch of a major European financial institution.

Iran has also established opaque shell companies in offshore jurisdictions. By incorporating these entities, and often obfuscating their corporate link to their real owner, Iranian companies maintain access to reputable banking services. Local payments, as noted earlier, elicit less concern and will frequently stay under the radar of sanctions enforcement authorities.

EXPLOITING LOOPHOLES

For Iran, sanctions are temporary roadblocks, not insurmountable obstacles. By building bypass roads, Iran turns crisis into opportunities. Iran's response to U.S. oil sanctions offers a case in point.

Section 1245 of the National Defense Authorization Act for Fiscal Year 2012[49] imposed secondary sanctions against Iran's oil exports. However, U.S. legislators made an exception for countries that would demonstrably reduce the purchase of Iranian oil over time. Iran's oil deliveries would then be purchased with local currency and placed in local escrow accounts, which Tehran could only access to purchase non-sanctioned goods from local companies. The money could not be repatriated.

Six countries adhered to this mechanism: China, India, Japan, South Korea, Turkey, and South Africa. Thus, Iran's oil revenues were locked in yuan, rupees, yen, won, lira, and rand, and only accessible for local purchases of approved goods.

These measures, while ensuring that the global oil markets remained stable, quickly depleted Iran's foreign currency reserves. Iran responded by establishing front companies in all six jurisdictions. Iran used these entities to circumvent Section 1245's provisions, and to serve as ATM machines. Classic money laundering techniques like over-invoicing and false invoicing enabled front companies to access the locked-up cash in local transactions. Payments to these companies could then be converted into foreign currency and moved to Iran, or made available to other Iranian overseas operations, as needed, for purchase of other goods.

A significant portion of the revenue was reinvested into gold and other precious metals and jewels, which are convenient substitutes for foreign currency. During 2012-2013, Turkey's sales of gold to Iran skyrocketed. The Iranians apparently recognized that gold sales to individual gold traders was authorized under the sanctions regime, so long as the stated destination was not the

[49] National Defense Authorization Act For Fiscal Year 2012, Pub. L. 112-81, codified as amended at 112 U.S.C., §1245. (http://www.treasury.gov/resource-center/sanctions/Programs/Documents/ndaa_publaw.pdf)

government of Iran. With Turkish help, Iran exploited this "golden loophole" [50] to the tune of $12 billion in the first year.

The loophole was ultimately addressed when Congress prohibited gold exports to Iranian government entities in U.S. legislation that passed in January 2013. Curiously, the Obama administration delayed the enactment of the law until July 2013, enabling the "gas-for-gold" scheme to continue for six more months.[51]

Iran responded with sophistication to U.S. sanctions against its petroleum exports by leveraging its access to the Turkish market. Since the passage of Section 1245, the number of Iranian companies in Turkey has grown exponentially – from 2,300 in November 2012 to 4,624 in December 2017.[52] Among them are numerous regime-affiliated companies suspected of sanctions evasion schemes.[53]

Iran has also evaded financial sanctions through remittance networks and currency exchange providers. These services help Iran launder money before it is repatriated or transferred to accounts overseas that Iranian proxies access for procurement purposes.[54] Because they are small, they are often harder to track – making them essential tools for Iranian financial sanctions evasion. In her November 2013 testimony to Congress, then-Financial Crimes Enforcement Network Director Jennifer Shasky Calvery noted that such tools are an ideal money laundering method, and not just for Iran, because they offer anonymity and usually elude custom controls. Unlike banking transactions, they leave almost no digital footprint.[55]

Many of the aforementioned cases of sanctions evasion included remittance providers. The Iranian network in Tbilisi that took control of Invest Bank JSC included money exchange businesses

---

[50] Gary Clark, Mark Dubowitz and Rachel Ziemba, "Iran's Golden Loophole," *Roubini Global Economics & Foundation for Defense of Democracies,* May 13, 2013. (http://www.defenddemocracy.org/content/uploads/documents/FDD_RGE_Iran_GoI_Report__May_2013_FINAL_2.pdf)

[51] Mark Dubowitz and Jonathan Schanzer, "Iran's Turkish Gold Rush," *Foreign Policy*, December 26, 2013. (http://foreignpolicy.com/2013/12/26/irans-turkish-gold-rush/)

[52] Republic of Turkey, Ministry of Economy, "FDI" accessed June 28, 2018. (https://www.economy.gov.tr/portal/content/conn/UCM/uuid/dDocName:EK-253303)

[53] U.S. Department of the Treasury, Press Release, "Treasury Targets Procurement Networks and 31 Aircraft Associated with Mahan Air and Other Designated Iranian Airlines," May 24, 2018. (https://home.treasury.gov/index.php/news/press-releases/sm0395)

[54] For an overview of these informal money networks and how money can be laundered through them, see: Financial Action Task Force, "Money Laundering Through Money Remittance and Currency Exchange Providers," June 2010. (http://www.fatf-gafi.org/media/fatf/ML%20through%20Remittance%20and%20Currency%20Exchange%20Providers.pdf)

[55] Jennifer Shasky Calvery, "Statement of Jennifer Shasky Calvery, Director Financial Crimes Enforcement Network United States Department of the Treasury," *Testimony before the Senate Committee on Banking, Housing, and Urban Affairs, Subcommittee on National Security and International Trade and Finance Subcommittee on Economic Policy*, November 19, 2013. (https://www.fincen.gov/news/testimony/statement-jennifer-shasky-calvery-director-financial-crimes-enforcement-network)

incorporated in Tbilisi, Dubai, Toronto, and Delaware;[56] three prepaid credit card companies[57] (one in Dubai, one in Tbilisi, and one both in Georgia and Iran);[58] an offshore online private banking company in New Zealand,[59] and another in Switzerland;[60] and a gold trader in Dubai.

According to a March 2015 Reuters report, over the course of several months in late 2014, money exchange businesses in Dubai helped Iran launder and exchange $1 billion in Emirati dirhams that were ferried across the Gulf by money couriers.[61] These schemes continue. Last May, working with authorities in the United Arab Emirates, Treasury moved to designate a Dubai-based money exchange network that laundered money and procured bulk cash in dollar denominations to Iran's Revolutionary Guard.[62]

Prepaid cards – another business that Iranian regime proxies have embraced – are a more contemporary, convenient version of traveler's checks. A variety of card types allow for reloading of funds; card-to-account, account-to-card, and card-to-card transfers; and worldwide cash withdrawals through ATM machines.[63] Numerous Iranian financial cross-border operations have offered prepaid cards among their products for years.[64]

Iranian companies offering online trading and high-end investment services are also becoming more frequent, especially in offshore jurisdictions like the Cayman Islands, Malta, Switzerland, and Uruguay.

FRAUDULENT PRACTICES

---

[56] New York Exchange LLC was sanctioned on February 6, 2014:
U.S. Department of the Treasury, Press Release, "Treasury Targets Networks Linked to Iran," February 6, 2014. (http://www.treasury.gov/press-center/press-releases/Pages/jl2287.aspx)

[57] Orchidea Gulf Trading LLC and its Turkish subsidiary were sanctioned on February 6, 2014: U.S. Department of the Treasury, Press Release, "Treasury Targets Networks Linked to Iran," February 6, 2014. (http://www.treasury.gov/press-center/press-releases/Pages/jl2287.aspx); Invest Bank Business Card Services Company LLC (http://www.companyinfo.ge/en/corporations/404399806/) was in all likelihood forcibly closed by Georgian authorities.

[58] "Travel Card FlyGeorgia," *Facebook*, accessed June 28, 2018. (https://www.facebook.com/TravelCardFlyGeorgia)

[59] "New York Fund Limited," *OpenCorporates*, January 5, 2015. (https://opencorporates.com/companies/nz/4062438); Corporate filings for New York Fund Ltd can be accessed at New Zealand's Companies Office website: http://www.business.govt.nz/companies/app/ui/pages/companies/4062438.

[60] EOT European Oil Traders SA was sanctioned on February 6, 2014: U.S. Department of the Treasury, Press Center, "Treasury Targets Networks Linked To Iran," February 6, 2014. (http://www.treasury.gov/press-center/press-releases/Pages/jl2287.aspx)

[61] Jonathan Saul, Parisa Hafezi, and Louis Charbonneau, "Exclusive: Iran smuggles in $1 billion of bank notes to skirt sanctions - sources," *Reuters*, February 24, 2015. (http://www.reuters.com/article/2015/02/24/us-iran-dollars-exclusive-idUSKBN0LS1LV20150224)

[62] U.S. Department of the Treasury, Press Release, "United States and United Arab Emirates Disrupt Large Scale Currency Exchange Network Transferring Millions of Dollars to IRGC-QF," May 10, 2018. (https://home.treasury.gov/news/press-releases/sm0383)

[63] See: Financial Action Task Force, "Guidance for a Risk-Based Approach: Prepaid Cards, Mobile Payments, and Internet-Based Payment Services," June 2013. (http://www.fatf-gafi.org/media/fatf/documents/recommendations/guidance-rba-npps.pdf)

[64] See, for example, Kiasun Card (http://www.kiasuncard.com/), and the associated Kiasun Exchange (www.kiasunexchange.com), which also trade in cryptocurrencies.

Iranian procurement and illicit finance activities face a 21st-century dilemma: how to disguise themselves in a digital world where information is difficult to conceal. The answer for them has been to hide in plain sight. Efforts by IRISL to elude sanctions are a case in point.

IRISL was sanctioned in 2010 under UN Security Council Resolution 1929.[65] Many of its subsidiaries had already been targeted by U.S. sanctions in 2008. To evade sanctions, IRISL incorporated a parallel structure of companies in Hamburg, all called "Ocean," numbering them from First to Sixteenth. Each "Ocean" had an "Administration" – First Ocean GmbH & Co. KG, First Ocean Administration GmbH – and all could be traced back to an Ocean Capital Administration GmbH. The parent company, in turn, traced back to IRISL.

Once this corporate structure was established, each company took ownership of IRISL ships. Vessels kept changing names and flags to elude further detection. Once the network was exposed, the U.S. Treasury had to include the International Maritime Organization number of each ship to ensure that each burdensome new designation would not be deferred or neutralized by Iran simply painting its vessels' names over the previous one.[66]

Transshipment (shipping goods to an intermediate destination, where new paperwork for the merchandise is produced before transporting it to another location) enables Iran to obfuscate the final destination of the merchandise it procures, especially via free zones. In 2014, for example, eight refrigerating units suitable for underground facilities were sold by an Italian subsidiary of a U.S. company to a Turkish contractor, ostensibly for a sport facility in Central Asia. Italian authorities, however, blocked the shipment at the port on suspicion that the machines were destined to Iran and constituted a WMD proliferation risk.[67]

Another case involved the aforementioned MCS International GmbH, which sent a shipment of gas cylinders to Golden Resources Trading Co., a Dubai-registered company. Authorities inspected the cargo, but – based on its documentation identifying the end user as a Dubai-based trading house – released it. The U.S. Treasury later sanctioned the trading house as part of a network of companies controlled by EIKO.[68] Golden Resources Trading's main function was allegedly to take consignment of the merchandise, prepare new paperwork showing Dubai as its origin, and then transfer it to Iran.

---

[65] United Nations Security Council, "Security Council Imposes Additional Sanctions on Iran, Voting 12 in Favour to 2 Against, with 1 Abstention," June 9, 2010. (https://www.un.org/press/en/2010/sc9948.doc.htm)

[66] For further details of Iran's shipping shell game, see: Claudia Rosett, "Iran Sanctions: A Tale of Two Fleets," *Forbes*, February 27, 2012. (http://www.forbes.com/sites/claudiarosett/2012/02/27/iran-sanctions-a-tale-of-two-fleets/); Claudia Rosett, "How Iran Steams Past International Sanctions," *The Wall Street Journal*, July 12, 2012. (http://www.wsj.com/articles/SB10001424052702303919504577522431458614636); Claudia Rosett, "Have Tehran Tankers hijacked Tanzania's Flag?" *Forbes*, July 12, 2013. (http://www.forbes.com/sites/claudiarosett/2013/07/12/have-tehrans-tankers-hijacked-the-tanzanian-flag/)

[67] "Rapporti Tra Accesso C.D. Difensivo E Documenti Coperti Dal 'Segreto' A Tutela Di Interessi Pubblici," *JUSforYou.it*, February 7, 2014. (http://www.jusforyou.it/main/?MID=1.4707.4714.4857&b=25248)

[68] U.S. Department of the Treasury, "The Execution of Imam Khomeini's Order (EIKO) International Financial Network," accessed June 22, 2015. (http://www.treasury.gov/resource-center/sanctions/Programs/Documents/eiko_chart.pdf)

Iran also resorts to simple tricks. Iran's network in Georgia used similarly named companies to make them harder to track. Its companies included names such as "Invest Fund Management," "New York Exchange," "New York Fund," and "New York Shipping." Another set of companies used the "Merchants Savings and Loans" label, which came in multiple variations, such as "Offshore Financial Company" or "Group."

Brand appropriation is another common practice. Rather than burying their company records under millions of Google search entries bearing similar word combinations, Iranian fronts link themselves to names, logos, and branding of credible financial and commercial institutions. This enables them to boost their credibility and give an aura of legitimacy to their operations.

ANCILLARY SERVICES

All of Iran's sanctions-busting activities rely on a service industry that enables Iranian agents, proxies, and intermediaries to conduct business in the most discreet way possible. This discretion can be achieved through the systematic acquisition of foreign passports. Iranian nationals routinely come under added scrutiny at border controls and financial institutions. Tehran's answer to this challenge has been to seek passports of convenience for its procurement agents, to enable undetected travel and, when needed, to relocate permanently to foreign jurisdictions to establish businesses that cannot be traced back to Iran.

The growing trend of citizenship-by-investment programs has created an opportunity for Iranians seeking to travel and conduct business overseas. There is now a growing number of available citizenship and permanent residency options available in return for real estate or business investments.[69]

The aforementioned case of Mehdi Shamszadeh is a good illustration: As reported by *Kayhan London*, Iranian officials instructed him to seek British citizenship to better facilitate his sanctions evasion activities.[70] Ali Sadr, the chairman of Malta's Pilatus Bank, who was recently arrested upon entry into the U.S. and indicted for money laundering and sanctions evasion,[71] held a St. Kitts and Nevis citizenship. So did the three Iranians implicated in the aforementioned Georgia network. And just recently, a Reuters investigation revealed that more than a hundred Iranians, many of them government officials, obtained Comoros Islands passports under a citizenship-by-investment scheme designed to attract foreign investment in the island nation.[72]

---

[69] The Dubai-based, Iranian-owned Capital Immigration LLC is one of the most comprehensive platforms for permanent residency or citizenship-by-investment programs. "About Us," *Capital Immigration Website*, accessed June 29, 2018. (http://www.capitalimmigration.net/ci_h.html)

[70] Potkin Azarmehr, "On Trial in Iran: A Dual National Accused of Stealing $40 Billion," *Kayhan London* (UK), July 10, 2017. (https://kayhan.london/fa/1396/04/19/on-trial-in-iran-a-dual-national-accused-of-stealing-40-billion)

[71] Nate Raymond, "U.S. arrests Iranian over alleged $115 million sanctions evasion scheme," *Reuters*, March 20, 2018. (https://www.reuters.com/article/us-usa-iran-crime/u-s-arrests-iranian-over-alleged-115-million-sanctions-evasion-scheme-idUSKBN1GW32E)

[72] Bozorgmehr Sharafedin and David Lewis, "Special Report: As sanctions bit, Iranian executives bought African passports," *Reuters*, June 29, 2018. (https://www.reuters.com/article/us-iran-passports-comoros-specialreport/special-report-as-sanctions-bit-iranian-executives-bought-african-passports-idUSKBN1JP14Y)

Iranian front companies have used offshore jurisdictions such as Panama, Liechtenstein,[73] the Channel Islands[74] and the Isle of Man,[75] the British Virgin Islands,[76] and Malaysia's Labuan.[77] To avoid detection, Iranian fronts relied heavily on the principle of beneficial ownership. The purpose of such practices is to obfuscate the real ownership of businesses that, if directly linked to Iranian citizens, might attract scrutiny or denial of banking services or licenses.

Ownership transfer is also routinely used to evade sanctions. The case of Babak Zanjani, Shamszadeh's senior associate illustrates the practice. In 2010, Zanjani established Kont Group, a holding company in Turkey. Kont Group established a holding company in Dushanbe, Tajikistan, and bought a local bank. The bank, Kont Bank Investment,[78] controlled a bank in Labuan, Malaysia, which was renamed First Islamic Investment Bank.[79] According to the U.S. Treasury, the two financial institutions were used to facilitate financial transactions by Iran's oil industry. Eventually, the EU sanctioned Zanjani and his network of companies in December 2012.[80] The U.S. followed suit in April 2013.[81] However, twelve days after EU sanctions were imposed, Kont Group appointed Turkish national Merve Irmak as managing director and soon thereafter, Zanjani transferred all his shares to Irmak. The new ownership of Kont Group was extended to its subsidiaries. In May 2013, the Dushanbe-based Kont Investment Bank, now under the chairmanship of a former Iranian Bank Mellat official, issued a press release declaring U.S. sanctions "unfounded" due to the new ownership structure at Kont Group.[82]

CONCLUSION

Mr. Chairman, Iranian attempts to obfuscate and conceal illicit procurement and sanctions evasion activity follow established patterns and share common features. Financial institutions and intelligence practitioners can use these typologies to identify actors and transactions that are

---

[73] KSN Foundation, sanctioned by the U.S. Treasury on February 6, 2014, is a Liechtenstein-based foundation.
[74] Naftiran Intertrade Company LTD, under U.S. and EU sanctions, was originally registered in Jersey, Channel Islands, before being moved to Switzerland and, subsequently, to Labuan, Malaysia.
[75] IRISL registered vessels in the Isle of Man: Allan Urry, "Why did Iran register ships in the Isle of Man?" *BBC News* (UK), July 14, 2010. (http://www.bbc.com/news/10604897)
[76] Pearl Energy Company LTD, a front for Bank Mellat, was sanctioned in June 2010 by the European Union: The Council of the European Union, "Council Decision 2011/299/CFSP," *Official Journal of the European Union*, May 23, 2011. (http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32011D0299)
[77] Pearl Energy Services LTD, a front for Bank Mellat, was sanctioned in June 2010 by the European Union: Council Decision 2011/299/CFSP of 23 May 2011 amending Decision 2010/413/CFSP concerning restrictive measures against Iran, *Official Journal of the European Union*, May 23, 2011. (http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32011D0299)
[78] "Welcome to Kont Bank," *Kont Bank Investment Website*, accessed June 22, 2015. (https://www.kontbank.tj/)
[79] "First Islamic Services," *First Islamic Investment Website*, accessed June 22, 2015. (http://www.first-islamic-bank.com/Default.aspx)
[80] Council Implementing Regulation (EU) No 1264/2012 of 21 December 2012 Implementing Regulation (EU) No 267/2012 Concerning Restrictive Measures Against Iran, *Official Journal of the European Union*, December 21, 2012. (http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2012:356:0055:0060:en:PDF)
[81] U.S. Department of the Treasury, Press Release, "Treasury Targets Network Attempting to Evade Iran Sanctions," April 11, 2013. (http://www.treasury.gov/press-center/press-releases/Pages/jl1893.aspx)
[82] Zarina Ergasheva, "Kont Investment Bank: U.S. Treasury Department's Actions Unfounded," *ASIA-Plus* (Tajikistan), February 5, 2013. (http://news.tj/en/news/kont-investment-bank-us-treasury-department-s-actions-unfounded)

potentially harmful to the integrity of the financial system or pose challenges to international security.

The Treasury Department plays a key role in this regard. Its sanctions and designations over the years have helped name and expose Iranian efforts to circumvent sanctions. But as my testimony indicates, this is a cat-and-mouse game, where one can never assume that countermeasures are the final word. Once designations are announced, we must assume that Iran will seek a way around them. **A constant update of sanctions and rigorous enforcement is therefore a key part of Treasury's ongoing effort.**

Congress, for its part, should strongly consider updates to the Bank Secrecy Act (BSA), which requires reporting of suspicious activity and transactions. The BSA legislation was first passed in 1970 and amended in title 111 of the USA PATRIOT Act. It needs to be updated to combat emerging trends in money laundering, including new forms of value transfer. With new and emerging payment systems, including virtual currency and mobile payment platforms, it is essential our regulatory regime keeps pace.

Iranian networks have always preferred procurement in Europe to Asia, and they have relied on Turkey and Gulf countries as transshipment points for their networks. **It is critical that Treasury leverages secondary sanctions to deter malfeasance in friendly jurisdictions.**

Europe needs to take a stronger stance against Iran and its proxies the IRGC and Hezbollah. The IRGC is reportedly involved in ballistic missile procurement throughout Europe and must be held accountable for this destabilizing behavior. The IRGC has gone so far as printing fake currency in order to finance their operations.[83] **Congress should encourage Europe to designate all of Hezbollah as a terrorist entity and continually investigate the IRGC and their investments.**

In the past year, the U.S. has sanctioned foreign banks, companies, exchange houses, shipping assets, and individuals for providing money and services to the IRGC and Hezbollah. The U.S. should continue these designations to put pressure on these terror proxies to limit their ability to use the formal financial sector. In addition, **law enforcement must continue to crack down on sanctions evaders that operate on the black market and in areas of high corruption.**

The most egregious money laundering networks feed off areas of low governance, such as the Tri-Border region between Argentina, Paraguay, and Brazil. **Congress should continue to resource the important work of the Drug Enforcement Administration, Department of Justice, the Coast Guard, and Treasury** as they take on this daunting task. Investigations of complex money laundering and sanctions evasion require significant time, and Congress should ensure that the resources provided match the scope of the problem.

Better transparency laws and regulations are needed in the United States and worldwide. Transparency is a powerful tool against Iranian efforts to procure technology and evade financial sanctions. The recent push by the United Kingdom and the European Union to require more transparency on the issue of beneficial ownership of companies is an important start. Jurisdictions

[83] U.S. Department of Treasury, Press Release, "Treasury Designates Large-Scale IRGC-QF Counterfeiting Ring," November 20, 2017.(https://www.treasury.gov/press-center/press-releases/Pages/sm0219.aspx)

such as Delaware and the Marshall Islands regrettably lack the necessary transparency to reduce the risk for sanctions evasion.

Finally, **the United States should address Iran's abuse of foreign passports by denying access to the visa-waiver program to any country that sells its citizenship for investment.** Of course, exceptions can be made for countries that are willing to share, on an ongoing basis, updated lists of beneficiaries of these programs as well as their due diligence packages.

These are some of my recommendations, Mr. Chairman. Thank you for the opportunity to testify and I look forward to your questions.

Center for a
New American
Security

July 12, 2018

Testimony before the House Financial Services Committee Subcommittee on Terrorism and Illicit Finance

Countering the Financial Networks of Weapons Proliferation

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

Thank you, Chairman Pearce and Ranking Member Perlmutter, for convening this hearing on countering the financial networks of weapons proliferation and for inviting me to appear before this subcommittee.

The financing of weapons of mass destruction proliferation is a grave threat facing the United States and the global financial system. The ability of rogue states and, potentially, malicious non-state actors to obtain weapons of mass destruction by using illicit financial activity and procurement networks is a major challenge to U.S. foreign policy goals, to the security of our homeland and that of our allies and partners, and to the integrity of the global financial system and the global nonproliferation regime.

Countering proliferation finance must be a core part of the policy approach to the United States' most pressing national security concerns, specifically North Korea, Iran, and Syria. Furthermore, the United States must lead on this issue in international forums such as the United Nations Security Council. This body and several others have taken important, though merely nascent, measures to place obligations on member states to halt proliferation finance. There is broad opportunity for the United States to advance policy and global cooperation on an important security issue, with near-term and meaningful benefits for global nuclear security.

Advancing the critical, even essential, global policy regime to counter the financing of proliferation will feature several primary challenges. First, proliferation finance is difficult to detect. Proliferation networks and specific individuals in these networks leverage the openness and interconnectedness of the global financial and trading system to achieve their malicious goals. For example, in 2013 Spanish authorities intercepted a shipment of corrosion-resistant valves destined for an oil field services company in the United Arab Emirates. Subsequent investigation found that the valves were going to be diverted to Iran for potential use in Tehran's nuclear program.[1] As evident from this case study, the global financial system prizes frictionless transfers of goods and capital, which

[1] Jonathan Brewer, "Study of Typologies of Financing of WMD Proliferation, Final Report," (Project Alpha, King's College London, October 13, 2017), https://projectalpha.eu/final-report-typologies-of-proliferation-finance/.

proliferators have taken advantage of on multiple occasions. Moreover, proliferators have taken advantage of gaps in different national regulatory regimes to evade detection. For example, although paragraph 16 of U.N. Security Council resolution 2321 (2016) requires U.N. member states to limit the number of bank accounts held by DPRK Embassy staff, the U.N. Panel of Experts on DPRK noted that states differed in their interpretation of the range of staff covered by this provision.

Second, countering the financing of proliferation is a highly technical subject, sitting at the intersection of sanctions enforcement, export control, financial crimes compliance, and the global nuclear nonproliferation regime. As these networks operate across multiple jurisdictions, involve an array of different constituencies—with different legal and regulatory authorities, various privacy and data-sharing obligations, and with major differentiation in political will and technical capacity—coordinating a truly effective international response is difficult. Many countries that otherwise lead on financial transparency and nuclear nonproliferation have struggled to summon the political will to tackle proliferation finance head-on, and even where there is political will government authorities and private sector compliance professionals may lack knowledge about how to do this work properly.[2]

It is truly alarming that the community of nations concerned by the threat of nuclear challenges, notwithstanding the ostensible commitment of many nations to this issue through support of multiple U.N. Security Council resolutions, nevertheless pays relatively less attention to the low probability but extraordinary high impact threat—the use of a weapon of mass destruction—than to the threat of a terrorist attack. While larger international financial institutions may have the resources and know-how to examine their transactions for the footprint of financing of proliferation, smaller, regionally-focused banks may not. Indeed, in some cases these smaller institutions may not even be aware of their obligations under international law, particularly if the local regulatory environment is weak.

The undeniable difficulties associated with countering the financing of proliferation, however, should not give the false impression that creating a more effective policy framework is beyond the capacity of the international community. We know the deficiencies in the system, and we can identify strategies to ameliorate them.

To begin with, there are major gaps in the regulatory regime that hamper a better response to this critical issue. Compliance and oversight programs for financial institutions have historically focused on financial integrity threats other than proliferation finance, like anti-money laundering, anti-corruption, and countering terrorist financing. This focus has led to a less-than-optimal outcome for checking the ability of North Korea and Iran, for example, to develop nuclear weapons capabilities. For policy leaders to clarify that counter-proliferation finance is on par with an obligation to counter terrorism will go a long way to raise the profile of this issue and update compliance posture.

Beyond a compliance footing, there are significant expertise and sophistication gaps in tracking proliferation financing not just among banks, but also among jurisdictions. While the United States,

[2] See e.g., Andrea Berger, "A House Without Foundations: The North Korea Sanctions Regime and Its Implementation," Whitehall Report 3-17 (Royal United Services Institute, June 2017), 40, https://rusi.org/sites/default/files/201706_whr_a_house_without_foundations_web.pdf.

the United Kingdom, and other European countries like France and Belgium have invested in building the institutional and intellectual capital needed to understand and counter this threat, many vulnerable jurisdictions such as Hong Kong or Malaysia have only recently begun to do so, and many more jurisdictions have not yet faced the issue. These countries will require more education and technical assistance, which the United States and a few in Europe, as well as Australia, are well positioned to provide. Some U.N. agencies offer workshops on proliferation financing (often together with terrorist financing), funded by countries such as Canada and Japan. Capacity building is important: as proliferation finance networks operate globally, and are quite adaptable, international efforts to combat them are only as strong as the weakest jurisdiction.

Given the size and reach of the U.S. financial system, as well as the sophistication of the legal and regulatory tools at the disposal of U.S. officials, Washington's policymakers must lead the way on disrupting the financing and procurement of weapons of mass destruction. U.S. policy leadership will yield numerous dividends. Not only will better regulation of the U.S. financial system foreclose avenues of proliferation finance in the United States, and via the U.S. dollar anywhere else in the world, but it will also offer important models for other jurisdictions to follow. Better U.S. rules can serve as standards of excellence for other jurisdictions and for financial institutions around the world. Global regulators and banks already look to the United States as the regulatory standard-setter for numerous aspects of the international financial system. A strong counter proliferation finance regime must be a part of that.

Expanding Mechanisms for Information Sharing

Perhaps the most significant policy adaptation that will help to counter the financing of proliferation is the crafting of better mechanisms for the timely collection and dissemination of information. Governments and banks must be able to share relevant information with one another or risk regularly, if unwittingly, facilitating the financing of proliferation. Banks must be able to widely, though securely and with appropriate data protections, share the information they collect relevant to proliferation finance through their routine business operations. Because most proliferation networks extend across multiple countries, individual jurisdictions, enforcement agencies, and financial institutions can acquire only a partial view of any one proliferation network. In one example of a prominent North Korean proliferation network, the web of trusted associates had operational nodes in China, Hong Kong, Malaysia, and Singapore.[3] Ensuring that policymakers can create the regulatory framework, nationally and internationally, to connect these partial perspectives, and thus successfully map international networks, will be critical to addressing this threat.

There are examples for information sharing in U.S. law that Congress, the administration, and U.S. allies and partners can build on. Sections 314 (a) and 314 (b) of the USA PATRIOT Act can serve as models for creating the operational ability to facilitate information sharing both between government and financial institutions and between financial institutions. These approaches, though, are only starting points. Many stakeholders claim significant concerns around different privacy regimes that prevent seamless sharing of information across national borders. Policymakers should

[3] Jonathan Brewer, "The Financing of Nuclear and Other Weapons of Mass Destruction Proliferation" (Center for a New American Security, January 2018), 7, https://s3.amazonaws.com/files.cnas.org/documents/CNASReport-ProliferationFinance-Finalb.pdf?mtime=20180202155127.

identify how to harmonize privacy regulations so that justifiable concerns about misuse of personal data do not prevent cooperation on an important law enforcement and international security priority.[4]

Better information sharing and data analysis tools can make the most of the data the U.S. government and counterparts already collect. Suspicious Activity Reports (SARs) generated by banks across the world for their regulators are an important source of insight into global proliferation finance networks. Congress should explore the development of new ways to gather and analyze this data in order to aid investigators in uncovering proliferation finance networks. There are new technology tools, including the application of machine learning and artificial intelligence methodologies, that may be of use. The United States can pilot fusion cells of experts with access to SAR and other relevant data (such as shipping data, travel records, or other sources) to experiment with new methodologies and technology for uncovering proliferation finance.

If policymakers pursue better information sharing mechanisms, or data analytics, solely in the United States, however, their effectiveness will be limited. Proliferation finance networks can span multiple jurisdictions so other major financial centers like Hong Kong, or major proliferation conduit jurisdictions such as Malaysia and Singapore, will need to adopt similar approaches to ensure the timely collection and use of information. It is encouraging that important U.S. partners, like the United Kingdom, are pioneering their own efforts to facilitate the sharing of sensitive information through its Joint Money-Laundering Intelligence Taskforce (JMLIT). Many jurisdictions have only started to work on how to incorporate best practices from these efforts into their own local policy and regulatory framework.

U.S. technical assistance can play a critical role in a process of replicating successful information sharing or analytical processes. Observers around the world have highlighted the utility of efforts by the U.S. Export Control and Related Border Security (EXBS) and the Defense Threat Reduction Agency (DTRA) programs to-date. The U.S. government should encourage and prioritize the provision of technical assistance to counterparts in jurisdictions with less-developed proliferation finance controls to expand relevant data and typology gathering, and strategies for producing proliferation-related red flags and SARs. Congress has an important role to play in funding and overseeing this strong and effective work. Legislators concerned with a comprehensive and successful approach to addressing North Korean and Iranian proliferation concerns, for example, must focus on proper resourcing and funding for these initiatives.

The Need for More Awareness-Raising

As previously noted, many countries and firms exposed to proliferation finance risk are unaware of this threat and their legal obligations to counter it. The U.S. government can foster efforts to better counter proliferation finance by offering more information to the public about the dangers facing the global financial system. Advisories by the Financial Crimes Enforcement Network (FinCEN) are invaluable in educating a wide variety of financial and legal sector stakeholders about threats to the

[4] See e.g., Andrea Berger and Anagha Joshi, "Countering Proliferation Finance: Implementation Guide and Model Law for Governments," Guidance Paper (Royal United Services Institute, July 2017), 23, https://rusi.org/sites/default/files/201707_rusi_cpf_implementation_guide_and_model_law_berger_joshi_0.pdf.

global financial system. By making more information available to financial institutions and outside experts, policymakers can also help create a virtuous cycle. More information from the government will lead to more useful and targeted detection of proliferation finance from the banks, which, in turn, will lead to even better information shared by the government. This entire process will lead to stronger law enforcement outcomes to counter proliferation finance and a stronger deterrent to proliferators to engage in this illicit activity in the first instance.

Policymakers must do more to release information about proliferation finance typologies to the public and key financial institutions and counterpart regulators. Outside experts have conducted useful work in this space that has significantly informed financial institutions' approach. Dr. Jonathan Brewer's "Study of Typologies of Financing of WMD Proliferation" serves as a valuable example of private study of these networks.[5] Similarly, the reports of the United Nations Panel of Experts created pursuant to Resolution 1874 have shone a light on global proliferation networks and offered an invaluable stream of information to banks seeking to shut these networks out of their institutions.[6] However these efforts are partial. Policymakers can significantly augment them by disclosing greater information about typologies of the financing of proliferation either in the public domain or through classified or private networks.

Law Enforcement and Disruption of Proliferation Finance Networks

Law enforcement will play a key role in any successful framework to counter proliferation finance. Over the past eight years, due to the attention paid to Iran and North Korea as proliferation threats, the U.S. law enforcement community has garnered an international reputation for its ability to investigate, disrupt, and prosecute those who operate proliferation finance networks. These professionals have unique strengths in asset tracing, compiling of typologies to dissect how proliferation finance networks have operated, and identifying shell companies to learn the true beneficial owner behind proliferation activities.[7]

Often, disruption of facilitation, including financial facilitation, networks is the preferred strategy of U.S. law enforcement officials when they are involved in work to counter proliferation. This is the case because many of the criminal actors in proliferation networks reside in jurisdictions outside of the reach of U.S. criminal prosecution. Asset seizure or forfeiture may also be an effective tool to raise the cost of doing this illicit business. Of particular utility are civil asset forfeiture authorities, and the 981(k) provisions which allow the United States to restrain, seize, and forfeit funds held in

[5] Brewer, "Study of Typologies of Financing of WMD Proliferation, Final Report."
[6] See especially "Report of the Panel of Experts established pursuant to resolution 1874 (2009)," United Nations Security Council (UN document S/2017/150), February 27, 2017, https://www.securitycouncilreport.org/atf/cf/%7b65BFCF9B-6D27-4E9C-8CD3-CF6E4FF96FF9%7d/s_2017_150.pdf and "Report of the Panel of Experts established pursuant to resolution 1874 (2009)," United Nations Security Council (UN document S/2018/171), March 5, 2018, https://www.securitycouncilreport.org/atf/cf/%7b65BFCF9B-6D27-4E9C-8CD3-CF6E4FF96FF9%7d/s_2018_171.pdf.
[7] See, for example, the Department of Justice's investigation of Dandong Hongxiang Industrial Development Co. Ltd. (DHID). "Four Chinese Nationals and China-Based Company Charged with Using Front Companies to Evade U.S. Sanctions Targeting North Korea's Nuclear Weapons and Ballistic Missile Programs," United States Department of Justice, September 26, 2016, https://www.justice.gov/opa/pr/four-chinese-nationals-and-china-based-company-charged-using-front-companies-evade-us.

foreign bank accounts located abroad by seizing an equivalent amount of funds in correspondent bank account of that foreign financial institution located in the United States. Put another way, this provision allows U.S. law enforcement to disrupt criminal activity even in jurisdictions with which the United States does not have extradition treaties. Here too international efforts will be important. In other jurisdictions authorities have faced difficulties and delays in carrying out seizures and freezes quickly.[8]

Financial System Transparency

Congress has a direct role to play in improving the legal and regulatory framework to counter proliferation finance. As a first priority, Congress should increase transparency in the financial system, and there must be no anonymous companies. This work is essential to arresting the ability of illicit proliferation networks to abuse our financial system to advance their dangerous work.

The recent introduction of H.R. 6068, "the Counter Terrorism and Illicit Finance Act," can be a step forward in reform of the Bank Secrecy Act to empower the administration to put in place strong counter proliferation finance strategies. It allows the sharing of suspicious activity reports within a financial group across international borders. However, in providing an 18-month safe harbor for violations of the customer due diligence rule it walks back existing supervisory expectations according to which regulators have been citing banks for years. It is indeed important to encourage financial institutions to self-report without fearing harsh legal action, but lawmakers must not water down existing practices related to customer due diligence, particularly the need to clearly determine customer activity and risk profile, that are so important—and must be built upon--to preventing illicit finance and abuse of the financial system.

Beyond this legislation Congress should partner with enforcement authorities to create incentives for U.S. financial institutions to innovate in their countering proliferation finance practices. Offering safe harbor from enforcement liability for financial institutions that demonstrate innovative approaches in their financial integrity controls is one potential incentive. Currently, the Bank Secrecy Act contains safe harbor from civil liability for Suspicious Activity SARs and Section 314 disclosures. Congress should ask the U.S. Treasury Department to develop safe harbor options to spur banks to allocate greater resources to information sharing and more effective analysis. The Financial Services Information Sharing and Analysis Center (FSISAC), which provides shielding and liability protection to members from certain regulatory requirements such as the Freedom of Information Act (FOIA), offers one model. While less beneficial to banks, Justice Department Cooperative Agreements may be another way in which financial institutions can receive credit for their cooperative efforts with government. Regulatory "sandboxes" that allow experimentation in countering proliferation finance while shielding institutions from liability are yet another means to incentivize private-public collaboration.

Given the importance of greater transparency to effectively counter proliferation finance, it is regrettable that Congress has not acted more swiftly in requiring complete and total disclosure of beneficial ownership information in regulations governing corporate entity creation. There must be no anonymous companies in the United States. While the report to be generated under Section 10 of

[8] Berger, "A House Without Foundations."

H.R. 6068 would provide useful information about how criminal investigators use the limited beneficial ownership information they currently collect, the requirements of the bill do not spur any immediate action to cut off proliferators and other illicit actors from the ability to create innumerable shell and front companies to disguise their criminal activity. If countering North Korea's and Iran's proliferation networks are truly top priorities of this Congress, legislators should consider requiring more concrete action on beneficial ownership in the short term.

Congress should also expand the amount of information required in financial payment messages. Lawmakers should also initiate a formal process with international counterpart parliamentarians to push for complementary requirements abroad. Many proliferators, along with other criminals, omit information incident to a transaction, and these data are only verified in a limited manner. Additionally, proliferators often use open account trade transfers, which, compared to letters of credit, convey only the most basic information about the purposes of a transaction and the parties involved, and which can often be falsified. The amount of information required in payment messages currently is insufficient to assist with countering proliferation finance investigations and to realistically protect financial system integrity.

Deepening Oversight of Non-Bank Commercial Institutions

In practice, the current countering proliferation finance regime relies on bank compliance to generate actionable intelligence. In particular, it does not well integrate other sources of trade or shipping data which could clarify and present opportunities for interdiction earlier in the supply chain. At present, banks may be able to eventually track proliferation products through retroactive investigation of transaction data, but they have virtually no ability to catch or interdict this commerce in real time. Shifts in the conduct of global trade finance, in particular the shift from letters of credit to open account transactions—have exacerbated this reality. The chance for disrupting proliferation finance exists when proliferation activities are identified before the final exchange of money and goods, which is difficult to do with open account transfers. Additionally, the amount of information conveyed is much less with open account transfers as compared to trade finance funded transactions.

U.S. policymakers can spearhead changes in global trade practices that may diminish the window of opportunity for proliferation networks. Today, the lack of standardized classification of goods and information included in trade and shipping documents is an information gap that both banks and governments confront. Too often inconsistent labeling can allow proliferation goods to slip through import-export controls. In my research on proliferation finance I have found that banks say these inconsistencies make it difficult to move with certainty in flagging suspicious trading activity. Closing this information gap by standardizing the taxonomy for goods within and across jurisdictions will ensure better customs compliance and enforcement, including through machine-driven screening and analytics across data sets, and it will help prevent labeling which obscures the real products being shipped.

In addition to the problem of labeling inconsistency, another core challenge to countering proliferation finance work associated with trade and shipping data is the inadequate supply of such financial documentation to banks. At present, regulatory requirements or cross-industry data-sharing mechanisms do not exist to close this gap. However, many stakeholders note that more, and more

consistent, trade information could provide critical insight for financial institutions screening, analyzing, and ideally disrupting, proliferation-linked transactions and networks. More cross-industry information sharing and more information in payment messages, both mentioned previously, can help address this issue.

The U.S. Presidency of the Financial Action Task Force (FATF), which began on 1 July 2018, is an invaluable opportunity for the United States to promote these critical issues within the framework of FATF, and to leave as its legacy a global financial system significantly strengthened against the threat of proliferation financing.

Working with U.S. allies and partners

Almost all global financial centers, particularly those in East Asia at the front lines of countering North Korean proliferation activities, are only beginning to acknowledge and understand the nature of the proliferation finance threat. Many of these jurisdictions are contemplating how to issue guidance on proliferation finance based on their own experiences with investigations and collection of data from SARs, as well as the development of information sharing mechanisms based on models used in the United States and the United Kingdom.

Financial institutions the world over will be key partners for policymakers in identifying the financing of proliferation. Institutional risk assessments will help inform this process and large, international banks who can do this work should pursue it aggressively and model it for smaller, regional banks who are at high risk. The increased use of risk assessments will be to the advantage of the non-proliferation regime, and the big banks, who have correspondent relationships with the smaller banks. As a result, it will make the whole system safer. The U.S. Congress can raise the flag on this issue in oversight of the executive branch and in the statements members make on how policymakers in the United States and abroad should address proliferation finance.

I want to close by stating how important it is for governments and financial institutions to avoid complacency over operations that might implicate North Korean and Iranian proliferation interests. The broader financial services and national security communities must understand that compliance with sanctions is insufficient on its own to counteract the activities of proliferation finance networks or to safeguard the integrity of the global financial system. The consequences for failing to appreciate the seriousness of the threat are real. International financial institutions face risk of expensive enforcement measures and the reputational harm that would come from facilitating transaction by rogue states. Governments face the risk of being the weak link that gives a WMD capability to a U.S. adversary. The stakes could not be higher.

Thank you for your time and attention. I look forward to your answering your questions.

Written submission to the United States House of Representatives
Committee on Financial Services
Subcommittee on Terrorism and Illicit Finance hearings
"Countering the Financial Networks of Weapons Proliferation"
12 July 2018

Jonathan Brewer, Adjunct Senior Fellow, Center for a New American Security, Washington, DC, and Visiting Professor, King's College London

1. Thank you Chairman Pearce and Ranking Member Perlmutter for inviting me to appear before you. I regret not being able to do so and hope this written statement will be helpful to your enquiries. The statement is focused on strategies to disrupt the financing and procurement of weapons of mass destruction, on how financial institutions can identify the financing of proliferation activities, and on the scope and effectiveness of relevant enforcement actions brought by various Cabinet Departments to counter proliferation financing, including the Departments of Justice, Treasury, Commerce and Homeland Security.[1]

Background

2. WMD proliferation can be carried out by States or by terrorist groups. State-sponsored WMD proliferation involves a range of industrial activity including construction and maintenance of in-country infrastructure and equipment, and management and administration of the technical workforce. Most WMD programmes also need to procure equipment and materials from overseas (particularly if their industrial or resource base is limited). Overseas WMD procurement networks may be elaborate, comprising front companies and individual agents, extending over several continents, and structured so as to obscure the end-users of equipment and materials that are sought and the sources of funds to pay for them. The network set up by Pakistani scientist A Q Khan,[2] which

[1] Topics listed in the Chairman's letter of invitation of 3 May 2018.
[2] See for example Nuclear Black Markets: Pakistan, A Q Khan and the rise of proliferation networks, International Institute for Strategic Studies, London, Strategic Dossier 2007.

became public in 2003, is best known although other elaborate networks have been prosecuted by US and other authorities.

3. Like all industrial activity WMD proliferation needs to be paid for, yet very few States try to attack procurement funding channels. "Following the money", a recognized tool to track financial crime, is rarely used to counter WMD proliferation. It should be used more.

4. The international community's primary tools to address the threat of WMD proliferation are UN Security Council resolutions. These impose requirements for action by every UN Member State. Resolution 1540 (2004) is intended to prevent proliferation by non-State actors (such as the elements of the AQ Khan network, or terrorists). The Security Council can also impose sanctions or other controls on state-sponsored proliferation programs (such as those of Iraq, DPRK or Iran). Other WMD programs may be the target of unilateral sanctions (imposed by the EU, US or other countries). The Syrian program is an example. The core of such sanctions is usually prohibitions on transfers of proliferation-sensitive equipment and materials, in order to slow or stop technical progress. They are usually implemented by individual states in the form of export controls.

5. However, these controls are not in themselves sufficient to guarantee the security of the international community from the threat of proliferation or its financing. First, not every potentially threatening WMD program is subject to sanctions (there are no sanctions on India's or Pakistan's programs) and although some states implement export controls focused on such programs, or on transfers of proliferation-sensitive equipment and materials more generally, these usually focus on stopping transfers of items rather than on their financing. Second, to get around sanctions or export controls, proliferation networks often exploit jurisdictions whose financial or export control systems are perceived as weak or easy to circumvent, or jurisdictions with political, trade, commercial/financial or historical links to countries with WMD programs.[3] So even though national authorities or financial institutions may argue that they have no exposure to proliferation financing risk (for example because they have no direct business dealings with states with proliferation programs), they

[3] See for example the 2012 Report if the UN Panel of Experts established pursuant to resolution 1874 (2009) (UN Document S/2012/422).

may still be exposed through business with banks or with companies that do, or business conducted in States nearby or where proliferation networks are active.

6. The theme of this testimony, which is based on published research,[4] is the need for the US, a recognized leader of international efforts to combat WMD proliferation, to persuade overseas jurisdictions to implement and enforce better systems to combat the financing of proliferation. This needs to be done bilaterally, through multilateral institutions such as the Financial Action Task Force (FATF) and by leveraging the role of the financial sector.

The practical problems of countering the financing of WMD proliferation

7. **Proliferation finance is difficult to identify**. WMD procurement financial transactions are usually difficult to distinguish from legitimate international trade and the number of such transactions is small in comparison. This is also true of terrorism financing, yet by comparison with terrorism financing little work has been done on proliferation financing typologies. FATF produced a report in 2008.[5] The Alpha Project at King's College London published a collation of case studies provided by national authorities and financial institutions in 2017 (research funded by US Department of State).[6]

8. **Proliferation finance is given low priority.** International organisations such as the G7 and UN have not treated proliferation finance with the same high priority as terrorist finance. The international framework to control proliferation financing is much less developed. In consequence most national authorities devote their energies to other threats to financial

[4] Jonathan Brewer, The Financing of Nuclear and other Weapons of Mass Destruction Proliferation, Center for New American Security, 24 June 2018.
[5] FATF Proliferation Financing Report 18 June 2008 (http://www.fatf-gafi.org/publications/methodsandtrends/documents/typologiesreportonproliferationfinancing.html)
[6] Project Alpha King's College London Final Report in Typologies of Financing of Proliferation of Weapons of Mass Destruction, 13 October 2017 (https://projectalpha.eu/final-report-typologies-of-proliferation-finance/). Funded under US State Department Award S-LMAQM-16-GR-1138, 16 August 2016 – 31 July 2017.

systems. In turn, few regulators require financial institutions to look for and report proliferation finance transactions. As a result little information is publically available on the scale of the problem.

9. **Inadequate coordination within national authorities**. Information on proliferation financing may be held by financial authorities, customs authorities, intelligence agencies or other departments but few countries have effective systems in place to share information or coordinate action. Export control authorities focus counter-proliferation efforts on stopping shipments of physical goods and may not have the powers or resources to investigate their financing. Financial Intelligence Units (FIUs) or other financial authorities may prioritise work on other forms of financial crime or threats to financial stability.

10. The international community should be developing fresh strategies to combat the financing of proliferation. These should take into account:

    - The critical importance of factoring the threat of proliferation finance into national risk assessments. National authorities should prioritise the collection and assessment of information relating to proliferation financing, and implement measures to mitigate risk;
    - The need for effective national legislation to counter proliferation financing. The provisions should create an offence of financing of WMD proliferation, not simply the financing of prohibited exports (to enable countries through which financing networks pass to take action against the financial transactions, independent of the location of items involved). Regulatory expectations regarding proliferation financing need to match high expectations regarding money laundering and terrorist financing;
    - The need for sharing information between international partners. Jurisdictions should have systems in place to disseminate and protect information, including sensitive intelligence, received from partners. Such information could be shared bilaterally or on multilateral channels (for example the Egmont Group of Financial Intelligence Units (FIUs));
    - The need for a mechanism to share information (including intelligence) and coordinate action within national authorities, departments and agencies. The UK Restricted Enforcement Unit

(REU) is an example of an effective mechanism;[7]

- The need to share information with banks and financial institutions. This should include both lead information (perhaps de-sensitised intelligence) and also feedback on material provided to authorities by banks. A refrain from some US banks is that they cooperate willingly with law enforcement but receive no feedback, so cannot judge how better to support law enforcement efforts;
- National authorities should also disseminate public guidance on WMD proliferation finance and information on typologies. This will help raise awareness.

How financial institutions can identify the financing of proliferation

11. Given the issues outlined in paragraphs 6-9 above, many financial institutions question the extent to which they should be playing a role in countering WMD proliferation. They argue that exporters or traders should be on the front line of controls since they need to apply for licenses for exports of dual-use or other strategically sensitive goods, and so should have a better understanding of proliferation-sensitive equipment and materials. This view is understandable but misguided. All private sector entities that might be involved in proliferation finance should be committed to contributing to international peace and security. Second, although the front line of controls should indeed be manned by exporters and traders, in many jurisdictions export control legislation is deficient and weakly enforced. Third (as noted above), shipping networks and financial networks may pass through separate jurisdictions. In the latter case, banks may be the only potential source of information.

12. **Risk assessments.** Most financial institutions comply with financial crime (money laundering) legislation and sanctions using a mix of rules-

[7] The REU meets every two weeks. According to its website, "The Restricted Enforcement Unit regularly considers the latest intelligence relating to potential breaches of export controls or other exports of concern and coordinates action by its member departments. These actions can include alerting UK exporters to the activities of proliferators (Awareness), seizing goods (Enforcement), investigating potential breaches of UK export controls (Legislation) and informing the authorities in other countries of proliferation activities under their jurisdiction and encouraging them to take action against them."

based and risk-based procedures. They screen transactions against UN, US, EU and other sanctions lists to ensure compliance with proliferation-related targeted financial sanctions (although as noted above, WMD financiers circumvent targeted sanctions by operating through front companies and complex financial networks in multiple jurisdictions). Financial institutions comply with money-laundering regulations using risk-based transaction-monitoring systems, calibrated to match an individual institution's type of business and risk appetite. They are usually purchased from commercial vendors. Few banks incorporate proliferation financing risk indicators into transaction monitoring procedures.

13. **Screening for equipment and materials**. Some financial institutions are experimenting with systems to screen transactions to detect proliferation-sensitive materials and equipment. This is possible if banks are involved in trade finance, and so have access to documentation that can be checked for proliferation-sensitive materials and equipment. The majority of trade finance takes place in Asia,[8] so investment in these sorts of checks seems sensible given the proliferation threats in that region. However on a global scale most international trade (perhaps 80%) is conducted not on trade finance terms but on "open account" terms, settled by wire transfers.[9] The SWIFT messages relating to such transactions carry little or no information about the nature of the business, such as goods, shipping routes, etc, and there is little value in screening them.[10]

14. **Global reach of proliferation networks.** Given the scale and complexity of proliferation finance networks any one individual financial institution, if unwittingly involved in the transactions, is unlikely to be involved in the complete network, end-to-end. Some financial institutions argue that their internal transaction-level controls are therefore unlikely to enable them to identify such a network. They need information from authorities or other sources.

---

[8] International Chamber of Commerce, 2017, Rethinking Trade and Finance, An ICC Private Sector Development Perspective.

[9] Page 19, paragraph 6.1 (a) of "The Wolfsberg Group, ICC and BAFT Trade Finance Principles, " http://www.wolfsberg-principles.com/pdf/standards/Trade-Finance-Principles-Wolfsberg-Group-ICC-and-the-BAFT-2017.pdf.

[10] SWIFT (Society for the Worldwide Interbank Financial Telecommunication) is a financial messaging system used by the large majority of the world's financial institutions.

15. **What banks should do to support counter proliferation financing.** Many US financial institutions argue that their databases can be useful for analysis and investigation when combined with open source information or intelligence shared by governments.[11] US Treasury Under Secretary for Terrorism and Financial Intelligence Sigal Mandelker earlier this year encouraged financial institutions to "... come forward with information. The more information you provide to us, the better able we are to assist you in tracking and tracing illicit actors and preventing them from accessing your institutions".[12] The financial sector should be pro-active in providing information to US authorities. Banks and financial institutions should also provide information to overseas jurisdictions where banking secrecy restrictions allow. This will encourage and support efforts by overseas authorities to assess proliferation finance and implement systems to mitigate the risk, if not in place.

16. International banks and financial institutions should screen their business transactions not only against US sanctions lists, but all proliferation-related sanctions lists (such as the UN, EU and others). They should then do the following.

- Conduct an assessment of the risk to their business from proliferation financing, taking into account specific proliferation financing indicators. FATF guidance is available, as are lists of possible indicators.[13] Based on this assessment they should incorporate indicators of possible proliferation financing into existing anti-money laundering and counter-terrorist financing compliance systems, focused on customers, counterparties, correspondent banks and international trade transactions. Financial institutions that purchase commercial compliance systems should require vendors to incorporate proliferation finance indicators into their products.

- Ensure that effective channels of communications are established with authorities so that intelligence or other information can be incorporated

[11] Although not always available in digital format and so not easily incorporated into financial institutions' monitoring systems.
[12] U.S. Department of the Treasury Under Secretary Sigal Mandelker Speech before the Securities Industry and Financial Markets Association Anti-Money Laundering and Financial Crimes Conference, New York City, 13 February 2018.
[13] See footnotes 4 & 5 above.

securely into databases, or used to establish internal lists of high-risk individuals or entities. In the US such information is shared by authorities under Section 314a of the USA PATRIOT Act. In the UK it is shared within the framework of the Joint Money Laundering Intelligence Task Force (JMLIT). A few other countries have similar arrangements to the UK.

- Ensure that information can be exchanged with other banks. Combining information might enable identification of networks that, as noted above, due to complexities or scale, might not be visible to any one bank alone. In the US such information is shared under Section 314b of the USA PATRIOT Act. In the UK it is shared in the JMLIT framework. A few other countries have similar arrangements to the UK.

- Foreign banks must comply with the requirements of their US correspondents in order to maintain access to the US financial system. By incorporating proliferation financing checks into their own business procedures and requiring the same of their respondents, US banks will help spread effective counter-proliferation financing practices throughout the global banking system. Foreign banks in turn should submit Suspicious Transaction Reports (STRs) to their local regulators if proliferation finance is detected. These STRs should include the indicators of proliferation finance in order to assist investigations by local authorities (outside the US very few authorities have proliferation finance expertise). Where local legislation does not require such STRs banks should find other channels to alert authorities. As noted above, such actions will encourage overseas jurisdictions to compile data to assess the proliferation finance threat and to put in place measures to control it.

- Compliance and investigative staff do not need to be experts in WMD proliferation programs, but maintaining a general brief on global developments (by monitoring information from governments, academia and media) should be a central element of their job description. In particular they should know sources of specialist advice if needed (such as academic institutions and think tanks in Washington DC, London and elsewhere). Banks and financial institutions should also dedicate teams to investigate suspected proliferation finance transactions to help build in-house expertise.

17. None of these proposals require banks or other financial institutions to introduce new compliance and due diligence procedures. They involve

modifications to existing procedures, and so should not be unduly resource intensive.

Scope and effectiveness of relevant enforcement actions brought by various Cabinet Departments to counter proliferation financing, including the Departments of Justice, Treasury, Commerce and Homeland Security

18. The Department of Justice publishes annually a summary of selected export enforcement and other cases.[14] Some of these involve WMD proliferation and are a rich source of information about proliferation finance typologies. US Department of the Treasury publishes advisories that may relate to proliferation finance.[15] These are valued by US financial institutions.

19. No overseas jurisdiction can match the resources of the Department of Justice, nor the expertise of the officers involved. However in almost all cases the action has been brought primarily on export controls grounds with money laundering included if information is available about financing or funding of prohibited exports. Within the US legal system there is no offence of WMD proliferation financing as such.

20. FATF awarded the US the top rating for implementation of UN targeted financial sanctions related to proliferation ("high level of effectiveness") following the mutual evaluation review of the US in 2016.[16] No other country evaluated by FATF has achieved this rating. FATF noted close cooperation and coordination amongst US authorities, sharing of information and intelligence, and extensive outreach and guidance to financial institutions. FATF commended the U.S. for a leading role in promoting effective global implementation of targeted financial

[14] "Summary of Major U.S. Export Enforcement, Economic Espionage, Trade Secret and Embargo-related Criminal Cases (current version published 19 January 2018) https://www.justice.gov/nsd/page/file/1044446/download

[15] See for example FIN-2017-A007 of November 2, 2017, Advisory on North Korea's Use of the International Financial System (https://www.fincen.gov/sites/default/files/advisory/2017-11-02/DPRK%20Financing%20Advisory% 20FINAL% 2011022017.pdf)

[16] Anti-money laundering and counter-terrorist financing measures, United States. Mutual Evaluation Report, FATF, December 2016 (http://www.fatf-gafi.org/media/fatf/documents/reports/mer4/MER-United-States-2016.pdf)

sanctions. The US is therefore uniquely well-placed to encourage other governments to do more to combat proliferation financing.

21. The US intention to use its Presidency of FATF to enhance FATF's work to combat WMD proliferation financing is highly encouraging. US efforts will include prioritizing work to close the gap in its standards between measures against proliferation financing, and those against money laundering and terrorist financing; ways to address the full range of proliferation financing activities in addition to targeted financial sanctions; the risks associated with proliferation financing and policies and controls to address those risks; and criminalization of proliferation financing.[17]

22. In addition, US authorities should consider:
    - Publishing additional advisories relating to proliferation financing. These are helpful to banks and financial institutions, and could be based on case studies relating to proliferation financing described in the annual Department of Justice report;
    - Encouraging the Egmont Group of FIUs to circulate case studies and assessments of proliferation financing. This will help sensitise national financial authorities about the threat.

Final Word

23. Countering the financing of procurement networks is a crucial element in combating WMD proliferation. All members of the international community need to be part of this joint endeavor. The networks are too big for any one jurisdiction to handle on its own. At a national level, countering proliferation finance requires a form of public-private partnership involving national authorities (intelligence agencies and security policymakers, customs and financial authorities) and banks and financial institutions.

---

[17] Objectives for FATF – XXX (2018-2019) Paper by the Incoming President United States Presidency Priorities for the Financial Action Task Force (FATF) (http://www.fatf-gafi.org/media/fatf/content/images/Objectives%20for%20FATF-XXX%20(2018-2019).pdf).

24. WMD proliferation is likely to threaten international peace and security for the foreseeable future. The US is uniquely well-placed to lead the international response. US authorities should persuade overseas jurisdictions to implement and enforce better systems to identify and combat proliferation financing. This should be done bilaterally and by leveraging the role of the financial sector. The US Presidency of FATF is a crucial opportunity to cement in place effective international measures to counter WMD proliferation finance.

involvement of Iran's financial system in illicit activities. As a result, we recommend the re-imposition of FATF counter-measures against Iran.

The pie chart in figure 1 shows the fraction of countries that have scores exceeding 50 percent of the total, between 50 percent and 25 percent of the total, less than 25 percent down to a score of 0, and below a score of 0. Only two countries received more than half of the available points. About one-third of all countries achieved negative scores.

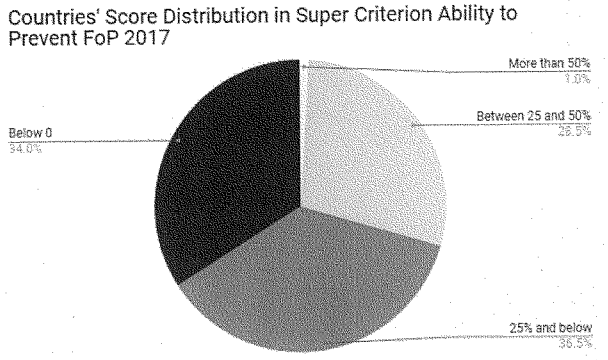

Figure 1. The pie chart shows the score distribution of countries in their *Ability to Prevent Proliferation Financing* in the PPI for 2017. The majority of countries score less than 25 percent of the available points. This figure includes corrected values for Viet Nam and Venezuela.

The PPI lists countries by score in the super criterion *Ability to Prevent Proliferation Financing*, which leads to a ranking. Although we do not release this ranking publicly, we provide below those countries that are in the top third and bottom ten percent by ranking.

Top third by rank (in alphabetical order):
Albania, Andorra, Antigua and Barbuda, Armenia, Australia, Austria, Bahamas, Bahrain, Barbados, Belgium, Bhutan, Botswana, Bulgaria, Burkina Faso, Cameroon, Canada, Chile, Cook Islands, Cyprus, Czech Republic, Denmark, Estonia, Fiji, Finland, France, Germany, Greece, Grenada, Hungary, Iceland, Ireland, Israel, Italy, Japan, Latvia, Lesotho, Liechtenstein, Lithuania, Macedonia, Malawi, Malta, Mauritius, Monaco, Nauru, Netherlands, New Zealand, Niue, Norway, Palau, Poland, Portugal, Romania, Samoa, San Marino, Singapore, Slovakia,

Slovenia, Solomon Islands, Spain, Sweden, Timor-Leste, Togo, Tonga, United Kingdom of Great Britain and Northern Ireland, United States of America, Uruguay, and Zambia.

Bottom 10% by rank (in alphabetical order):
Afghanistan, Belarus, Burundi, Democratic People's Republic of Korea (DPRK), Egypt, Eritrea, Iran (Islamic Republic of), Iraq, Lebanon, Libya, Morocco, Myanmar, Paraguay, Russian Federation, Serbia, Somalia, South Sudan, Sudan, Syrian Arab Republic, Thailand, and Ukraine.

Updates Since the Publication of the PPI 2017 regarding proliferation financing

Since the publication of the index, Institute staff have continuously updated and revised the data for a 2018 version of the ranking. Throughout the process, trends observed in the 2017 data on proliferation financing remain. Countries still perform poorly overall, and only three countries received 50 percent or more of the possible points.

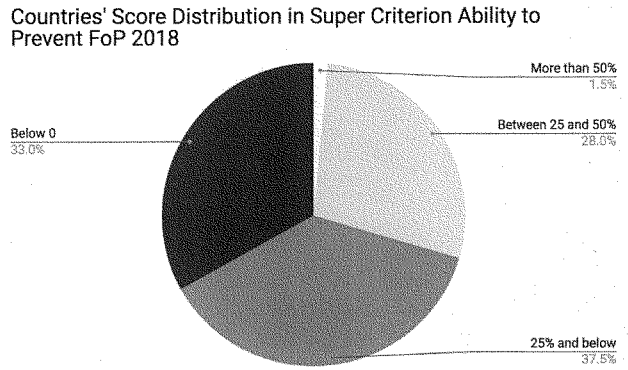

Figure 2. The pie chart shows the score distribution of countries in their *Ability to Prevent Proliferation Financing*, 2018 ranking. The majority of countries score less than 25 percent of the available points. In general, the distribution in these four broad categories has only minimally changed from 2017 and the need for further action is clearly visible.

As stated before, the PPI lists countries by score, generating a ranking. Although we do not release this ranking, we again provide those countries that are in the top third by ranking and the bottom ten percent in the 2018 ranking.

CONGRESSIONAL TESTIMONY: FOUNDATION FOR DEFENSE OF DEMOCRACIES

House Financial Services Committee
Subcommittee on Terrorism and Illicit Finance

Countering the Financial Networks of Weapons Proliferation

DR. EMANUELE OTTOLENGHI

Senior Fellow
Foundation for Defense of Democracies

Washington, DC
July 12, 2018

FDD
FOUNDATION FOR DEFENSE OF DEMOCRACIES

www.defenddemocracy.org