SAFEGUARDING THE FINANCIAL SYSTEM FROM TERRORIST FINANCING

HEARING

BEFORE THE

SUBCOMMITTEE ON TERRORISM AND ILLICIT FINANCE

OF THE

COMMITTEE ON FINANCIAL SERVICES

U.S. HOUSE OF REPRESENTATIVES

ONE HUNDRED FIFTEENTH CONGRESS

FIRST SESSION

APRIL 27, 2017

Printed for the use of the Committee on Financial Services

Serial No. 115–18

U.S. GOVERNMENT PUBLISHING OFFICE

27–419 PDF WASHINGTON : 2018

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

HOUSE COMMITTEE ON FINANCIAL SERVICES

JEB HENSARLING, Texas, *Chairman*

PATRICK T. McHENRY, North Carolina, *Vice Chairman*
PETER T. KING, New York
EDWARD R. ROYCE, California
FRANK D. LUCAS, Oklahoma
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

KIRSTEN SUTTON MORK, *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

SAFEGUARDING THE FINANCIAL SYSTEM FROM TERRORIST FINANCING

Thursday, April 27, 2017

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 2:23 p.m., in room 2128, Rayburn House Office Building, Hon. Stevan Pearce [chairman of the subcommittee] presiding.

Members present: Representatives Pearce, Pittenger, Rothfus, Tipton, Williams, Poliquin, Love, Hill, Emmer, Zeldin, Davidson, Budd, Kustoff; Perlmutter, Maloney, Himes, Foster, Kildee, Delaney, Sinema, Vargas, Gottheimer, Kihuen, and Lynch.

Ex officio present: Representatives Hensarling and Waters.

Also present: Representative Royce.

Chairman PEARCE. The Subcommittee on Terrorism and Illicit Finance will come to order.

Without objection, the Chair is authorized to declare a recess of the subcommittee at any time. Also, without objection, members of the full Financial Services Committee who are not members of the Subcommittee on Terrorism and Illicit Finance may participate in today's hearing.

Today's hearing is entitled, "Safeguarding the Financial System from Terrorist Financing."

I now recognize myself for 5 minutes to give an opening statement. Today, most of us are very fortunate to have a more modern and secure means of storage for our hard-earned money. Unfortunately, so do terrorists, cartels, and other criminals around the world. In an ever-evolving world, this is the driving mission of our subcommittee: How can we continue to provide the safety and security in our markets that American families have come to expect while rooting out the bad actors in the system? What actions is our Nation taking to ensure markets for legitimate users? What in our current AML/CFT structure is working and what needs improvement?

Today's hearing is the first in a series this subcommittee will hold on the Bank Secrecy Act and the regulatory structure the United States has in place to combat money laundering, terrorist financing, and other illicit financing activities. It is only fitting that the subcommittee begins its work by examining the role and the function of the Financial Crimes Enforcement Network, more com-

monly known as FinCEN, which was established in 1990 by the Secretary of the Treasury.

FinCEN was upgraded to official bureau status in 2002 with the passage of the PATRIOT Act. The bureau is not only the primary regulator of the BSA, but it also acts as the United States' financial intelligence units (FIUs). FinCEN's mission is to safeguard the financial system from illicit use and combat money laundering and promote national security through the collection, analysis, and dissemination of financial intelligence and strategic use of financial authorities.

From the most traditional forms of financial transactions to the ever-evolving world of financial technology, it is essential that our Nation has an efficient, effective, and modern set of rules and regulation to safeguard our Nation's financial system. This hearing starts the conversation and ensures our subcommittee is taking pragmatic and complete look at the laws and regulations we currently have in place.

I thank our witnesses for being here today and I look forward to the conversations to come.

With that, I will now recognize the ranking member of the subcommittee, the gentleman from Colorado, Mr. Perlmutter, for 5 minutes for an opening statement.

Mr. PERLMUTTER. Thanks, Mr. Chairman, for holding this hearing so our subcommittee can design policies to update, modernize, and strengthen the Bank Secrecy Act.

FinCEN plays a critical role in safeguarding our Nation's financial system through the collection and analysis of suspicious activity reports (SARs) and currency transaction reports (CTRs). In fact, FinCEN has collected over 200 million filings. The U.S. continues to be the financial capital of the world whereby essentially all payments move through or touch the United States' financial system. Therefore, the U.S. plays an important role in reducing the threat of terrorism and disrupting illicit and illegal financial flows. So it is important we evaluate how our current regulatory regime is functioning, what is lacking or needs updating, how we can better strike a balance between law enforcement and civil liberties, and how we can build in efficiencies without overburdening our financial institutions.

I want to thank Mr. El-Hindi for your testimony today.

Chairman PEARCE. If you will hold here, let me yield one of my minutes to Mr. Pittenger, and then that gives us a second there to—

Mr. PERLMUTTER. All right. I will yield.

Chairman PEARCE. Mr. Pittenger is recognized for 1 minute.

Mr. PITTENGER. Thank you, Mr. Chairman, and thank you, Ranking Member Perlmutter, for organizing such an important hearing and such a timely reason to meet with our Financial Crimes Enforcement Network.

Director El-Hindi, thank you for your excellent service and your friendship, and thank you for lending your time to our subcommittee today.

Earlier today, FinCEN associates of Mr. El-Hindi joined our subcommittee members and staff at a roundtable meeting with several major financial institutions to discuss the importance of informa-

tion sharing as a tool to combat terror finance. Specifically, we were discussing how Section 314 of the USA PATRIOT Act can be codified to improve the information-sharing process for our financial institutions. Information sharing for financial institutions is a critical component of our domestic capabilities to stop the flow of illicit funds to support terror, both domestic and abroad.

Director El-Hindi, thank you for your service. I look forward to hearing your testimony.

I yield back.

Chairman PEARCE. The gentleman yields back.

Mr. PERLMUTTER. I will yield the balance of my time back to the Chair.

Chairman PEARCE. Okay. And when we get an opportunity, we will try to recognize that.

Today, we welcome the testimony of Mr. Jamal El-Hindi, who has served since May of 2015 as the Deputy Director of the Financial Crimes Enforcement Network, or FinCEN, a bureau of the Treasury Department. Mr. El-Hindi has served at FinCEN in various positions since June of 2006. Prior to joining FinCEN, Mr. El-Hindi served as the Associate Director for the Program on Policy and Implementation at Treasury's Office of Foreign Asset Control, or OFAC. Mr. El-Hindi first joined Treasury in December of 2000 in the Office of General Counsel. Prior to that, he served as an associate at Patton Boggs in Washington, D.C..

Mr. El-Hindi graduated from the University of Michigan Law School, and received a master of arts in modern Middle Eastern and North African studies from the University of Michigan, a diploma in international relations from the London School of Economics and Political Science, and an undergraduate degree in journalism from the University of North Carolina.

Mr. El-Hindi, you will now be recognized for 5 minutes to give an oral presentation of your testimony. And without objection, your written statement will be made a part of the record.

And I recognize the gentleman from Colorado.

Mr. PERLMUTTER. Thanks, Mr. Chairman. I notice the ranking member has just joined us, and if I could have unanimous consent to—

Chairman PEARCE. Yes. The gentleman is recognized to yield time to the gentlelady from California.

Mr. El-Hindi, if you will suspend here for a second.

Mr. PERLMUTTER. I would like to yield to the ranking member of the full Financial Services Committee, the gentlelady from California, Ms. Waters, for her statement.

Ms. WATERS. Thank you very much. I appreciate your consideration. Thank you, Mr. Chairman.

One of the key issues this subcommittee will be looking at is the adequacy of current information-sharing authorities and the degree to which they strike the right balance between security and civil liberty concerns. Last Congress, we heard from a number of experts and Administration officials who spoke to the benefits and efficiencies that would accrue from increased information sharing between financial institutions and the government, as well as financial institutions themselves. But I would also like to note that nearly every expert who spoke in favor of improved information

sharing also acknowledged that these efforts must be cognizant of the need to protect privacy and civil liberties.

So, Mr. Chairman, as we explore legislative efforts to codify current authorities or otherwise enhance information sharing, I strongly agree that we have a responsibility to solicit views from all interested stakeholders, and we need to hear and discuss these views and concerns in a public setting, such as this hearing today, and not only in private meetings.

I would also like to touch upon another important issue, which is the gaping hole in our anti-money-laundering framework with respect to the real estate sector. While I appreciate, Mr. El-Hindi, that your written testimony notes the "outstanding concerns" that FinCEN has had with the money laundering risk in real estate, I must say that I find it disturbing that FinCEN continues to largely exempt the real estate sector from even the most basic anti-money-laundering requirements, given that high-end real estate is a key sector used by corrupt foreign leaders, drug traffickers, and other criminals to launder illicit money. I believe FinCEN should take more urgent action to address these risks nationwide and on a permanent basis.

And with that, I yield back the balance of my time. And thank you very much.

Mr. PERLMUTTER. I yield back. Thank you.

Chairman PEARCE. The gentleman yields back.

Now, Mr. El-Hindi, I will recognize you for 5 minutes.

STATEMENT OF JAMAL EL-HINDI, ACTING DIRECTOR, FINANCIAL CRIMES ENFORCEMENT NETWORK, U.S. DEPARTMENT OF THE TREASURY

Mr. EL-HINDI. Chairman Pearce, Vice Chairman Pittenger, Ranking Member Perlmutter, and the distinguished members of the subcommittee, thank you for inviting me to appear before you today to discuss the role of the Financial Crimes Enforcement Network in collecting, analyzing, and disseminating Bank Secrecy Act data. I appreciate the subcommittee's interest in FinCEN's mission and your continued support of our efforts. My oral remarks are brief. I am submitting a more comprehensive written statement.

FinCEN, as we are commonly known, is a Treasury Department bureau charged with safeguarding the financial system from illicit use, combating money laundering, and promoting national security through the collection, analysis, and dissemination of BSA information, and the strategic use of our authorities. We are one of five components reporting to the Under Secretary for Terrorism and Financial Intelligence collectively focused on Treasury's mission in this area.

FinCEN serves two roles. First, as the financial intelligence unit for the United States, we collect, analyze, and disseminate financial intelligence to help fight money laundering and the financing of terrorism. Second, we are the lead regulator for the Federal Government with respect to anti-money-laundering and countering the financing of terrorism, also known as AML/CFT.

FinCEN's ability to work closely with regulatory, law enforcement, industry, and international partners promotes consistency across our regulatory regime. In short, we strive for responsible use

of financial information for greater security and integrity in the U.S. financial system.

The Bank Secrecy Act is the primary Federal anti-money-laundering law. It requires a broad range of U.S. financial institutions to establish anti-money-laundering programs, maintain records, and provide reports to FinCEN. The majority of BSA data FinCEN collects comes from two reporting streams. Financial institutions must file currency transaction reports, known as CTRs, with FinCEN for cash transactions totaling more than $10,000. They must also file suspicious activity reports, known as SARs, to report suspected illicit transactions.

The objective reporting in CTRs and the subjective reporting in SARs are both critically important. They provide a wealth of potentially useful information to FinCEN and other agencies working to detect and prevent money laundering, other financial crimes, and terrorism.

Thanks to funding from Congress, FinCEN successfully completed an information technology modernization program in 2014 updating the process of collecting, analyzing, and disseminating BSA data.

FinCEN receives an average of roughly 55,000 new financial institution filings each day. These filings come from more than 80,000 financial institutions and 500,000 individual foreign bank account holders through FinCEN's modernized e-filing system. FinCEN maintains over 200 million of these BSA filings in our database. FinCEN makes this information available to more than 10,000 law enforcement and other government users through a search tool designed to meet their specialized needs. We call it FinCEN Query. Our users, internal and external, perform approximately 30,000 searches of the data per day.

E-filing has streamlined the reporting process for financial institutions and individual filers, and has significantly improved users' ability to exploit BSA data by making it more accessible and searchable.

The protection of the sensitive information received is a critical part of our mission. FinCEN safeguards BSA data through a continual process of reviewing IT security measures and procedures, adjusting to current and emerging risks, and ensuring that security is a consistent requirement considered throughout the life cycle of each system. FinCEN systems are accredited to high Federal information security management levels and employ strong security measures, such as two-factor authentication, encryption, and activity monitoring to protect BSA data.

FinCEN works with others in the Department of the Treasury and the Department of Homeland Security in its focus on cybersecurity within the general context of security operations and mitigation activities.

FinCEN delivers BSA information and related analysis to law enforcement, regulatory, foreign, and private sector partners following a five-stage cycle. The cycle involves: one, collection; two, data processing and exploitation; three, analysis; four, dissemination; and five, the direction of future BSA collection efforts.

In the first stage of the cycle, FinCEN not only collects the types of reports I mentioned previously, such as SARs and CTRs, but

also has the ability to collect other data. FinCEN can proactively target certain financial intelligence for collection using a variety of authorities and special measures that might involve focus on particular areas or financial institution.

Data processing and exploitation is the second stage of the cycle. With approximately 55,000 filings per day, advanced technology solutions are needed to review, analyze, and quickly disseminate time-sensitive information.

To combat our most significant money laundering and terrorist financing threats, FinCEN employs automated business rules to screen filings on a daily basis and identify reports that merit further review by analysts.

For the analysis and dissemination stages of the cycle, the third and fourth stages, over the past few years we have consolidated our analytic capabilities and expanded the scope of our work to create products that address critical priority threats for our stakeholders, including the financial industry.

With respect to dissemination in particular, financial intelligence is most effective when information flows in both directions between the public and private sectors. FinCEN is a critical hub between financial institutions, law enforcement, regulators, and international colleagues. Providing information back to the financial industry based on our analysis of their reporting is a force multiplier.

One of the tools FinCEN uses to disseminate information to industry is our financial institution advisory program. FinCEN can issue public and nonpublic advisories to alert financial institutions of specific illicit finance risks. Advisories often contain illicit activity typologies, red flags to facilitate monitoring, and guidance on complying with FinCEN requirements.

In addition to close collaboration with domestic partners, FinCEN works to establish and strengthen mechanisms for the exchange of information globally. We engage with, encourage, and support international partners to take steps to strengthen their own regimes. Much of this involves FinCEN's interaction with other financial intelligence units.

FinCEN and most other FIUs are members of the Egmont Group, through which we collectively serve as conduits for information requests from each other's law enforcement agencies.

The fifth and final stage of the intelligence cycle involves using everything we have learned to help inform future planning and direction. Once threats and vulnerabilities have been identified, FinCEN can adjust the regulatory framework protecting the U.S. financial system. FinCEN uses its regulatory rulemaking authority to, among other things, define the reporting that financial institutions and others must provide. These rulemaking activities, together with the special information collections and advisories I previously mentioned, expand or improve the information that FinCEN collects. The dovetailing of this final stage with the collection I outlined as the first stage confirms the iterative and cyclical nature of our financial intelligence activities.

I will conclude by noting that the annual CFT landscape is complex and dynamic. It requires ongoing adaptation by FinCEN and our many partners. As we have to adjust to ever-evolving threats, we will continue to use the tools at our disposal to collect financial

intelligence information, analyze it, and deploy it in support of our mission to safeguard the system from illicit use, and promote national security.

On behalf of all the hardworking and dedicated FinCEN staff, I want to thank you again for the opportunity to testify today, and I look forward to your questions.

[The prepared statement of Acting Director El-Hindi can be found on page 32 of the appendix.]

Chairman PEARCE. Thank you, Mr. El-Hindi.

The Chair now recognizes himself for 5 minutes for questions.

Mr. El-Hindi, on page 3, you talk about the number of filings each day, and those numbers seem very large. Of those filings, which ones actually turn into actionable information, just roughly?

Mr. EL-HINDI. In terms of trying to associate each filing with a particular action, that is a little bit difficult. I realize that the number of filings that we have is large, but you have to understand how it is used. The filings could be a tip in and of themselves alerting law enforcement to something that they hadn't known before. They can be used to expand law enforcement investigations. They are also used to identify trends in terms of what is going on in terms of the financial sector, and new methodologies with respect to illicit activity.

Chairman PEARCE. How many people do you have assigned to review these reports?

Mr. EL-HINDI. At FinCEN, we currently have on staff 280—

Chairman PEARCE. I am not asking the number on staff. I am asking the number of people who are directed to this. Surely you have some people who open the mail and who answer the phones to just walk-in traffic, so not every one of your people. How many are assigned to go through the 55,000 new filings every day?

Mr. EL-HINDI. At FinCEN, we have an intelligence division staff of approximately 70. But keep in mind that because we have 10,000 other users of the database throughout the government, there are others who are also looking at the information on a daily basis.

Chairman PEARCE. That gives me a scope of what I am looking at.

Now, on page 12, you are talking about the amount of money that you returned. Do you have estimates of how much is lost every year?

Mr. EL-HINDI. I think that you are referring to the portion in the written testimony where I talk about business email compromise. Just by way of background, that is a situation in which we have been working with the FBI to have reported to us situations in which someone has compromised an email account and directed a financial institution to send funds, maybe a payment or something else, instead of the usual place that it should go, to a new place to go.

The estimates of that type of fraud, business email compromise, are in the hundreds of millions. I don't have specific numbers on it.

Chairman PEARCE. Hundreds of millions a year or—

Mr. EL-HINDI. Yes.

Chairman PEARCE. Yes. Okay.

Mr. EL-HINDI. This is a phenomenon that has started over the past few years. So I think that is cumulative.

We have been able, through our contacts with other financial intelligence units, when we can alert them quickly to the fact that funds have fraudulently gone overseas, we have been able to work with them to have a transaction stopped and have money returned to the United States. Over the past year and a half, 2 years, we have been able to assist in the recovery of approximately $250 million.

Chairman PEARCE. Okay. You talk in your testimony about IT modernization. How long had you all been working on that, and did the modernization actually work? I ask that because, as a pilot, I watch the FAA and their continual attempts to change the way they process data, and it never works and it is always extremely expensive and it is always behind time. Give me a little bit of an update on that?

Mr. EL-HINDI. With respect to our modernization program, I think we do consider it complete. We are now in the operation and maintenance phase of continuing it. It was a program that was a multiyear effort, but we delivered it on time and under budget. And in terms of external review of it, it was one of those few situations where we got no recommendations from our auditors in terms of how we might have been able to—

Chairman PEARCE. So you feel satisfied with what you got?

Mr. EL-HINDI. Yes.

Chairman PEARCE. Okay.

Mr. EL-HINDI. We actually—I will say, there is always room—

Chairman PEARCE. All right. I don't need any qualifiers here.

The process does not appear to have undergone much change since you all were stood up as an organization. Does that process need review?

Mr. EL-HINDI. In terms of the premise of the question that the process hasn't changed much since we were stood up, I might disagree with that.

Chairman PEARCE. Okay.

Mr. EL-HINDI. I think that the rules and the requirements have pretty much stayed the same, but we collect information from the financial sector. The ways in which we have analyzed that information and begun to disseminate it and more actively target some of our information collection with industry have changed over the course of time.

Chairman PEARCE. Okay. My time has expired.

I will now recognize the ranking member, the gentleman from Colorado, for 5 minutes.

Mr. PERLMUTTER. Thanks, Mr. Chairman. And we have a lot of Members here today, so I am just going to focus on one subject and then yield back.

First, I would like to introduce into the record FinCEN–2014-G001, dated February 14, 2014, "BSA Expectations Regarding Marijuana-Related Businesses."

Chairman PEARCE. Without objection, it is so ordered.

Mr. PERLMUTTER. Thank you.

Mr. PERLMUTTER. So my focus is going to be, obviously, on marijuana. We are now at 29 States that have some level of medical

marijuana or fully legalized marijuana usage, plus eight or nine States with cannabis oil for seizures and other maladies. So today, I introduced the Secure and Fair Enforcement Banking Act, which was formerly the Marijuana Business Access to Banking Act, to try and get us here in the Congress to say if a State has a regulatory structure in place, then all of the different Bank Secrecy Act and SARs and things like that are sort of set to the side, and if individuals are operating as legitimate businesses in their State, then they will be given authority to continue to do business.

But my questions are to you, Mr. El-Hindi—and thank you for your service to the country—what is the status of the guidance that I just listed, otherwise known as the Cole memo? Are you going to follow it? That is my question.

Mr. EL-HINDI. The Cole memo actually came from the Department of Justice.

Mr. PERLMUTTER. Right.

Mr. EL-HINDI. And I will say—

Mr. PERLMUTTER. In concert with FinCEN.

Mr. EL-HINDI. And our guidance followed on that. The Cole memo specified some priority areas for law enforcement focus in the marijuana space. Our guidance was designed, within the financial sector space, to provide law enforcement with information that would be useful with respect to following those priorities.

We feel that the guidance has worked. There is information in the database that, under the guidance, helps financial institutions distinguish between situations in which they are providing service to a marijuana business where it seems to be consistent with the State law and does not touch upon any of the priorities in the Cole memo. That is one type of filing that they can do.

They can do a type of filing where they indicate that there are other activity—there is more suspicion—

Mr. PERLMUTTER. They are out of—there are irregularities of some kind.

Mr. EL-HINDI. Yes. And then they file reports when they have terminated the relationship as well.

The construct there actually came from what we saw the banks filing even prior to the guidance coming out. In a situation where you have a conflict of a Federal law and a State law, we wanted to see how the banks were actually dealing with it. And when we looked at the data that they had already been providing, they were making those distinctions in terms of situations where they would say, the only reason we are filing this suspicious activity report is essentially because marijuana trade remains illegal under Federal law.

So we saw the distinctions that they were making. We felt that going forward with guidance in the way that we did would provide law enforcement in States, whether legalized or nonlegalized, it would provide them with information that they could use.

In our context, for us, it is all about the information and making sure that law enforcement has the information that it needs.

We will continue to work with law enforcement and the Department of Justice on that front. And to the extent that they—you will provide any further indication of what their needs are, we will be working with them.

Mr. PERLMUTTER. So far, you are operating under that guidance that I read into the record?

Mr. EL-HINDI. That guidance still stands.

Mr. PERLMUTTER. Yes. Thanks.

I yield back.

Chairman PEARCE. The gentleman yields back.

The Chair now recognizes the gentleman from North Carolina, Mr. Pittenger.

Mr. PITTENGER. Thank you, Mr. Chairman. And thank you again, Mr. El-Hindi.

Mr. El-Hindi, just for clarity, your interest in FinCEN is to receive the data from the financial institutions, these SARs reports, and analyze this data and then send that out for certain investigations. Is that correct?

Mr. EL-HINDI. That is one of the many things that we do in terms of our support to law enforcement.

Mr. PITTENGER. In that framework.

Mr. EL-HINDI. Yes.

Mr. PITTENGER. What I would like to assess here is the impact that could be achieved by the banks also having access to data from the government and how that might limit or greatly restrict the number of potential SARs reports that need to truly be evaluated or to be processed out for investigation. Is that a good assumption?

Mr. EL-HINDI. I think that you are touching upon some of the work that we have been trying to do with industry and law enforcement to target information-collection efforts.

Mr. PITTENGER. Given the impediments that we have in terms of restrictions in data sharing, would it be reasonable to assume that we can achieve better results with less proactive engagement through a broad range of data over the financial institutions? If we had a safe harbor for banks where they could share with each other, and if they had access to government data, would that enhance our ability and make it a more fluid approach that would make us to not have to address as many data points as are acquired at this point?

Mr. EL-HINDI. I think the enhanced sharing of information across financial institutions, based on what we have seen and how we have worked with them, really would be helpful. Each of them only has so much of a view of a particular transaction. And some of the special projects that we have engaged with them, we have been quite happy to bring them together, have them share information with each other and share information with ourselves, and we do view that as bringing added efficiencies to our regime. The benefits with respect to that type of information sharing are clear.

Mr. PITTENGER. We heard this morning from Andrea Sharrin, your associate, and with a number of banks who were there who were wanting to achieve the best results but believe that we may have less interest—or less cause for privacy issues if we—through—if that data-sharing capacity was there, and that we wouldn't infringe on privacy issues as much if we would be able to enhance the data-sharing capabilities. Would you concur with that?

Mr. EL-HINDI. I think that the opportunities for greater data sharing among the banks and among the banks with government

are great. And I think that, as was mentioned earlier, we have to be sensitive to the privacy issues that come up both with respect to general reporting under our rules as well as with respect to information sharing among the banks.

Mr. PITTENGER. One other question quickly, as you work with other FIUs and the Egmont Group, what is your assessment in terms of their technological capabilities, admitted extraordinary software capabilities that are already there at FinCEN, do you believe that we need to do greater work with our allies and friends in terms of enhancing their technological capabilities to have better engagement with us and collaboration with us?

Mr. EL-HINDI. One of the things that we have been talking about within the FIU community generally is making sure that FIUs are well-positioned to do the work that they are supposed to be doing. Different FIUs in different jurisdictions are at different points, but as a group, we work on trying to elevate each other as much as possible. And there are ways in which some of them could benefit from greater capacities technologically as well as greater support within their own legal systems.

Mr. PITTENGER. But to the extent that they are weak, it weakens the entire system. Isn't that correct?

Mr. EL-HINDI. Yes. We always say that within a global system, the weakest link can hurt the chain.

Mr. PITTENGER. Yes, sir. Thank you.

Chairman PEARCE. The gentleman's time has expired.

The Chair now recognizes the gentlelady from New York, Mrs. Maloney, for 5 minutes.

Mrs. MALONEY. Thank you, Mr. Chairman, and thank you to the ranking member. And thank you to our witness for being here today.

You mentioned in your testimony that FinCEN issued two geographical targeting orders, or GTOs, covering two sites, Manhattan and Miami, that would require title insurers to collect beneficial ownership information for any legal entity making an all-cash real estate transaction over a 6-month period. And I am very pleased that FinCEN extended these GTOs in February, so I want to thank you and your organization for doing that. But the findings from the first 6 months were absolutely startling.

As you noted, about 30 percent of the transactions reported in those 6 months involved a beneficial owner or purchaser representative that had previously been the subject of a suspicious activity report. And I would say it is unusual to be buying real estate with all cash. It is usually in the banks and everything. So the fact that it is an all-cash transaction and that there also is a suspicious activity report, and 30 percent is really, I think, problematic. I would characterize it as a shockingly high number, especially since you announced to the world that you would be collecting this information on beneficial ownership in these two cities for that exact period of time. So I would think that money launderers or bad actors would just know not to go to those two cities during this timeframe, since it was so widely reported.

So in light of the findings from these two GTOs, would you say that collecting beneficial ownership information is important for

catching money launderers and stopping terrorism financing and other illegal activity like gun running or other illegal activities?

Mr. EL-HINDI. Yes. Beneficial ownership information and the collection of it and greater transparency in that space are definitely something that will help law enforcement in their efforts.

Mrs. MALONEY. And what do you think about the 30 percent who are using cash to—

Mr. EL-HINDI. Let me also clarify that in the context of the geographic targeting order, when we talk about a cash transaction in real estate, we are essentially saying, and we clarified this in the rollout of the GTO, that we were focused on non-loan-related transactions. The cash component of it comes into play with respect to the confines of our 8300 requirement and our geographic targeting order, generally.

The way the requirement works, if it is a non-loan-related transaction, and some portion of that transaction involved cash or a monetary instrument and was done by a legal entity and within the thresholds that we set with respect to the value of the property, then it was reportable.

So the geographic targeting order was very specific. There are certain things that would not be captured within that reporting, for example, an all wire transfer of funds, even though it was—there was no loan involved with a bank, would not have been covered by that geographic targeting order.

Mrs. MALONEY. There have been a number of reports in New York that real estate over $2 million is almost always an LLC. Beneficial ownership is hidden. Have you done any reports looking at LLCs, which is the prime form of hiding the ownership, the number of them in the country now? Could you look at it if you haven't?

Mr. EL-HINDI. I would have to get back to you in terms of precisely what our analysts might have researched. We are all familiar with some of the things that we see in the press reports. And real estate has been an area that we know that we need to focus on. It has been an evolutionary process for us.

I would just go back and say that with respect to how we have covered residential real estate in the past, since roughly 75 percent of the market involves a bank or a bank loan, we feel that the involvement of the banks in those contexts provides us with a certain amount of coverage, but we do have to focus on areas where banks aren't involved.

Mrs. MALONEY. Actually, we just came from a meeting that Mr. Pittenger organized, and the banks were saying they don't know the ownership either in an LLC. They have no idea.

So I just would just like to ask very quickly, do you think it would be easier if companies had to disclose the beneficial owners at the time the company is formed?

Mr. EL-HINDI. Yes. That kind of transparency would certainly be of benefit to law enforcement.

Mrs. MALONEY. As many people on this committee know, I have a bill that would do just that. So I want to thank you for your thoughts and input on it.

Mr. EL-HINDI. If it would be helpful, and to the extent that Congress is going to focus on this issue, we would be happy to work with them.

Mrs. MALONEY. Thank you very much. My time has expired.

Chairman PEARCE. The gentlelady's time has expired.

The Chair now recognizes the gentleman from Pennsylvania, Mr. Rothfus.

Mr. ROTHFUS. Thank you, Mr. Chairman. And thank you, Mr. El-Hindi, for being here today.

Talk a little bit more about these real estate transactions. Does the government have any idea of how many real estate transactions involve money originating from foreign accounts?

Mr. EL-HINDI. I would have to get back to you on that in terms of any work that we have done particularly in that context. I will say that the real estate market is complicated. It is something that varies, the information requirements and processing requirements vary by State, and vary by county. So it is something where we feel that we still are in the process of collecting information to find out precisely what information is out there and how we should approach it.

Mr. ROTHFUS. I may want to follow up with you on that.

Do you foresee a need to expand the use of geographic targeting orders to more localities in the U.S.?

Mr. EL-HINDI. The geographic targeting order authority that we have had, we have been using more of, of late, just as part of FinCEN being more active in this space. Law enforcement has asked us, and we have worked with them on geographic targeting orders in Los Angeles with respect to garment manufacturing. We have done work in Miami with respect to trade in electronics equipment, both of those on a trade-based money laundering context. It is a useful tool and it is something that we continue to explore the best use of with law enforcement.

If you are asking with respect to real estate in general, I am not in a position right now to talk about any future regulatory efforts. I can just tell you in general that we find the tool useful and continue to discuss it.

Mr. ROTHFUS. What about the 180-day duration of a GTO? Is that long enough?

Mr. EL-HINDI. To the extent that a GTO needs to be extended, we can extend it for another 180 days under the statute.

Mr. ROTHFUS. Do you know whether there would be certain domestic real estate markets that are exposed to cartel-owned real estate, real estate that the cartels from Latin America might be going to certain geographic regions?

Mr. EL-HINDI. I can tell you that in terms of some of the criteria that we looked at and discussed with law enforcement when we identified regions of focus, we were looking at the market, we were looking at to the extent that there was an active use of shell companies within that real estate market, we were looking at value, we were looking at the amount of foreign interest in those jurisdictions. So that is how we made selections in terms of the scope of the geographic targeting order.

Mr. ROTHFUS. The difference between our larger institutions and smaller ones, are smaller banks and credit unions more vulnerable to money laundering versus the bigger banks?

Mr. EL-HINDI. Small banks and bigger banks, they are both banks, they both process transactions. They have different ways of knowing who their customers are. I would say that both can be vulnerable, and that is why both are subject to our rules. We say that banks need to comply on a risk-based approach. They need to assess their risks and act accordingly.

I would just say that with respect to smaller institutions, for example in the terrorism context, some might assume that they may not have the same type of information that large banks might have, or be able to look at thousands and thousands of records, but we have seen that in the terrorism context, small banks are contributing, I think it is 10 or 12 percent of some of the most useful reporting in that regard.

There are differences among those institutions and there are differences in the way they approach things, but both large institutions and small institutions have a very important role in what we do.

Mr. ROTHFUS. I thank the gentleman.

I yield back.

Chairman PEARCE. The gentleman yields back.

The Chair notes that votes have been called. It is my intention that if Mr. Foster, who is next in the queue, desires to go ahead and ask questions now, we will do that. We will come back and complete the hearing afterwards, but you can go now or wait till after the votes, Mr. Foster. It is your choice.

Mr. FOSTER. I am happy to proceed.

Chairman PEARCE. Okay. The gentleman is recognized for 5 minutes.

Mr. FOSTER. Thank you for everything you do here. I would like to return to the real estate issue a little bit. You mentioned the value of just eliminating anonymous shell corporations, which is something—do you know roughly what fraction of countries on Earth allow anonymous shell corporations and what don't?

Mr. EL-HINDI. I do not have that information.

Mr. FOSTER. Would you feel comfortable in saying the majority do not allow anonymous shell corporations?

Mr. EL-HINDI. Again, I would have to—

Mr. FOSTER. Okay. I would be interested in knowing that, because it is my impression that we are sort of an oddity in allowing this, and it is the—makes—one of the reasons that the U.S. is not on the center for financial activity generally, but also unfortunately for a lot of money laundering.

The other thing, some countries, it is my impression, have what is often called a cadastre. This is a legally binding registry of who owns which parcel of land, so you can sometimes literally just go to the Federal map and mull over a certain plat of land, and it gives you the whole ownership history and all the transactions. This is information that is publicly accessible in the U.S., but often only by going into the basement of some dusty courthouse to get that information. And if there was a national legally binding registry of who owns which parcel of land—and I think some States

are doing this, for example, Minnesota, areas of Canada, I believe, do this—would that really simplify the whole procedure of figuring out what each transaction was about?

Mr. EL-HINDI. I would just say that in general, greater transparency with respect to beneficial ownership in this space would be useful. Precisely how we get there is something that, again, we would be happy to work with the Congress on to the extent that they are focused on this issue.

Mr. FOSTER. Now, you go through title insurance companies to attempt the geographical targeting. In what ways is that satisfactory or unsatisfactory or complete or incomplete?

Mr. EL-HINDI. When we looked at the geographic targeting orders, we were trying—and as we would do in any regulatory context where we are trying to collect information, we are looking for nodes and places where we can efficiently collect information. In that context, given their role in the transactions and the information that they could obtain as part of that, we felt that it made sense.

Mr. FOSTER. All right. And is title insurance mandatory for these cash transactions and so on?

Mr. EL-HINDI. I had mentioned before that what happens in each particular part of the country in terms of the jurisdiction—there are different rules in different places, whether it is mandatory, whether it is something that is essential—has become essential by virtue of practice, I would have to get back to you on. I just would say that part of the complications in the real estate sector is the variety of rules that exist.

Mr. FOSTER. Thank you. I think this is something where Congress should really have a look at this, because the anonymous ownership of land is—not only having to do with terrorist financing, but there is a lot of just ordinary corruption associated with secret ownership of land in this country. And it would be, I think, in the interest of good government, general governance generally to have some improvements here. So thank you.

I yield back.

Chairman PEARCE. The gentleman yields back.

It is the intent of the Chair to reconvene the hearing immediately after votes. For now, the subcommittee stands in recess.

[recess]

Chairman PEARCE. The subcommittee will come to order.

We will resume with questions. We left off with Mr. Foster from the minority side, and we will proceed to Mr. Williams from Texas.

You are recognized for 5 minutes.

Mr. WILLIAMS. Thank you, Mr. Chairman. And thank you, Mr. Director, for being here today.

I wanted to first start by exploring the topic of trade-based money laundering (TBML) this afternoon, then discuss in more depth the use of geographic targeting orders, GTOs as we know them, by FinCEN and the use of trade transparency units.

As you know, trade-based money laundering is a process in which someone, whether that be a criminal or terrorist organization, attempts to disguise the proceeds of crime, in this case using trade to legitimize their illicit behavior. And although it is difficult to put a price tag on how much money is laundered annually

through trade, I think it is safe to say it is in the billions of dollars. In fact, a 2010 advisory report on TBML issued by FinCEN stated that from 2004 to 2009, more than 17,000 suspicious activity reports described TBML involving transactions totaled $276 billion. And although the practice of TBML is common, combating it remains very difficult, especially when companies change names, locations, and schemes so frequently.

So let me start by asking you this: Is that normal? Is it routine for the names to change and the businesses to go on operating?

Mr. EL-HINDI. I would say that is definitely a methodology we have seen in some of our work and certainly with our work with law enforcement.

Mr. WILLIAMS. Okay. Is the U.S. Government not providing adequate resources to help you combat these schemes?

Mr. EL-HINDI. Congressman, I think that, as you have seen from the things that we have put out, we know that trade-based money laundering is an issue, and we continue to work on it and we work with financial institutions on it. We work with the trade transparency units as well. They have access to the data that comes to us through the financial institutions, and we work with them to make sure that they are in a position to use it. We have ongoing discussions with them on that. It is definitely an issue and it is something that we are focused on.

Mr. WILLIAMS. Do you think it is all about resources, or does Congress need to give more authority in this space?

Mr. EL-HINDI. I am really not in a position right now to talk about our authorities. I can just tell you that within the authorities that we do have, and the information that we are currently collecting, we are working with other parts of the government.

Mr. WILLIAMS. Okay. In your testimony, you spoke about GTO authority, which Congress gave Treasury the authority to use in the 1980s. And although back then, criminal organizations were mostly cash and other monetary instruments, wire transfers are not covered in the GTO authority. And as we had talked about in past hearings, and something that is personal to me as an auto dealer, the trade-based money laundering scheme using used cars relies heavily on money transfers for completing a sale. Do you believe Congress needs to go back and update this authority?

Mr. EL-HINDI. To the extent that Congress is interested in looking at that authority, and looking at some of the issues that have been raised with respect to the limits on what we are able to collect currently, we would be happy to work with Congress on that.

Mr. WILLIAMS. Good. In your opinion, what industry that GTOs are intended to target can circumvent these orders by using wire transfers?

Mr. EL-HINDI. I'm sorry. Could you repeat that?

Mr. WILLIAMS. What industry the GTOs are intended to target can circumnavigate these orders by using wire transfers?

Mr. EL-HINDI. To the extent that the authority right now is limited to our ability to use geographic targeting orders when there is cash involved, any type of transaction that goes through wire transfers wouldn't be within the scope of what we could do. So I would say that that is going to apply to a variety of different businesses.

Mr. WILLIAMS. Okay. Finally, something that this committee has talked extensively about expanding is the use of trade transparency units (TTUs) to help combat trade-based money laundering. Most of the active TTUs reside in countries located in South America. In addition, the importance of knowing trends and conducting ongoing analysis of trade data provided through partnerships with other countries, trade transparency unit is vital. I think we would agree.

So, Director, although FinCEN doesn't run these units, can you talk to the committee about the importance of sharing data with other countries and maybe how expanding these units will help you better do your job?

Mr. EL-HINDI. A lot of other parts of government that are focused on the TTUs address the TTU aspect of it. I can just tell you again that, domestically, we work with the TTUs and we are focused on making sure that they have the data that we have and they are able to use it. And then generally speaking, in terms of the way we as a financial intelligence unit work with our counterparts overseas, we have definitely been pushing for more and more appropriate sharing on a secure and efficient basis of the information that each of us have. So, I think in the FIU context, with respect to financial intelligence, we definitely see the value of working with our counterparts overseas.

Mr. WILLIAMS. Thank you for your testimony.

And I yield back.

Chairman PEARCE. The gentleman's time has expired.

The Chair now recognizes the gentleman from Minnesota, Mr. Emmer.

Mr. EMMER. I thank you very much. I want to thank you for being here today, and the chairman and the ranking member for setting this up.

As I understand it, you have been the acting Director—well, actually, not the acting Director. You have been the acting Director since the new Administration came in, of FinCEN?

Mr. EL-HINDI. I have been acting Director since—

Mr. EMMER. 2015?

Mr. EL-HINDI. I have been the Deputy Director since 2015, and in May 2016, I became the acting Director.

Mr. EMMER. Thank you.

FinCEN has how many total employees?

Mr. EL-HINDI. Onboard right now, we have about 280, and our target is 340.

Mr. EMMER. And your total budget, annual budget, is in the neighborhood of what?

Mr. EL-HINDI. Historically, it has been in the $110 million to $115 million range. I am not prepared to get into budget specifics right now.

Mr. EMMER. No. I was just asking for a ballpark, and it is nothing—these aren't "gotcha," whatever. I am just asking—

Mr. EL-HINDI. Thank you.

Mr. EMMER. —mostly for my own knowledge.

And you are divided up into six divisions, as I understand it?

Mr. EL-HINDI. Yes.

Mr. EMMER. And since you have been at FinCEN, has the organization been remodeled in any way or changed, or has this always been the way it has been since it was created?

Mr. EL-HINDI. Actually in 2013, we went through a restructuring of the organization under the previous Director. I was onboard at that point and I headed one of the divisions at the time. And that restructuring, we undertook because FinCEN, as I mentioned before, bridges the financial community, the law enforcement community, the regulatory community, and our international counterparts.

Mr. EMMER. Right.

Mr. EL-HINDI. And under our previous structure, we found that the divisions that were focused on regulatory seemed to view only the financial sector as their customers. The division that was focused on analysis and liaison only viewed law enforcement as their customers. A division focused on international issues only focused on other FIUs.

The reality is, for an organization like ours, every one of our stakeholders is a customer of the whole organization. And in the new structure, we tried to break that down a bit, and we really stressed the fact that every external stakeholder is a customer of every part of FinCEN and every part of FinCEN is a customer of every other part. So it is six divisions—

Mr. EMMER. If I can interrupt you, because I am going to run out of time. I am not interested—and forgive me if I sound a little sharp—in customers of FinCEN. I am more interested in you are collecting all this information, 154,000 reporting entities, which I would suggest you would call one of your customers if you are looking at this whole thing.

I am really concerned about private information and how you ensure that law abiding people are not drawn into this net: 55,000 reports every day based on suspicious activity. I was trying to look at the law. How is suspicious activity defined and who makes the determination as to whether it is suspicious or not?

Mr. EL-HINDI. With respect to the reporting that we get, keep in mind that some of it is the currency transaction reporting, which is objective reporting of the value of the transaction if it is more than $10,000 of cash coming in and out.

Mr. EMMER. Right.

Mr. EL-HINDI. That is objective reporting. That is roughly 15 million reports a year.

Suspicious activity is more subjective, and our regulations—

Mr. EMMER. Who determines it?

Mr. EL-HINDI. Our regulations instruct the bank.

Mr. EMMER. Yes. So you send out a guideline, right?

Mr. EL-HINDI. To the bank, yes.

Mr. EMMER. And what is your guideline—

Mr. EL-HINDI. Banks and other financial institutions.

Where they have reason to believe that the source of funds might be illicit, where the transaction might not seem to have an apparent business purpose—

Mr. EMMER. What happens if they don't—so what if they are just putting money into a savings account?

Mr. EL-HINDI. To the extent that an individual is putting money into a savings account, a bank might not find that suspicious.

Mr. EMMER. But it seems to be so vague. What is suspicious activity? And if you are putting the onus on the reporting institution, what is the consequence if they don't—

Mr. EL-HINDI. I understand. So let me just work through a story. Say, I am a customer of the bank—maybe I am a student; I am a student customer of the bank. The bank understands that I am a student and I have opened up an account. To the extent that as a student I begin to engage in incredibly large and repeated transactions, that is going to be something that the bank, in terms of knowing its customer and what it might expect from a student, would say, that looks suspicious. That is different from a transaction that you would normally expect from a student. That is just one category.

The guidance that we provide to banks walks through—helps them identify red flags in certain situations in which they could be identifying that type of activity.

Mr. EMMER. I see my time has expired. If I could get a copy of your guidance afterwards—

Mr. EL-HINDI. Sure.

Mr. EMMER. —I would appreciate it.

Mr. EL-HINDI. Of course.

Mr. EMMER. Thank you.

Chairman PEARCE. The gentleman's time has expired.

The Chair now recognizes the gentleman from Maine, Mr. Poliquin, for 5 minutes.

Mr. POLIQUIN. Thank you, Mr. Chairman, very much. And thank you very much for being here, sir.

You folks, in my terminology anyway, are the financial cops for the U.S. Government, intelligence and the cops. Is that right, roughly?

Mr. EL-HINDI. Yes. We assist. We assist the cops and—

Mr. POLIQUIN. Good.

Mr. EL-HINDI. —we assist the financial institutions.

Mr. POLIQUIN. Great. So we know how important your work is, Mr. El-Hindi. We are quite proud of our State of Maine. We consider ourselves one of the safest States, and statistically are one of the safest States in the country. However, all of us, I think, here in Congress have been alarmed by knowing that there are terrorist investigations going on in each of the 50 States, I should say. And one of the things that really frightened us last summer was, actually, an individual who had settled in Maine as a refugee ended up dying on the battlefield for ISIS in the Middle East. So we all want to make sure we help you make sure this process is as efficient as possible.

Now, Mr. Emmer and other folks have mentioned the huge volume of SARs every day, about 55,000. Based on 70 or 80 folks you have working on this at your shop, if I understand this, that is about 800 per day. So, that is a lot. And I am not quite sure. I am guessing it probably doesn't make a lot of sense to spend a lot of manhours on 800 filings per day. I am guessing some of those aren't of great quality.

And is there anything—and if I am wrong, I know you will correct me—that we can do to help you, any legislation we can pass, any rulemaking that you folks can go through with our support that allows you to use different technology to get to a better place so this is more efficient, to make sure we drill down on what filings are actionable?

Mr. EL-HINDI. I will just try to provide a little context with respect to all that information that comes in. It is varying types of information. As I mentioned before, some of it is objective reporting. Some of it is suspicious activity reports. And when you think about the percentage of things that come in on a daily basis, the percentage of SARs is actually going to be lower in comparison with currency transaction reports. That is just the math.

But people need to—we try to make sure that industry and the public understand that the way this information is used is in a variety of contexts. It is not easy to associate any one particular filing with any one particular action. In fact, in terms of our metrics and how we measure our success, we try to emphasize the fact that it is not as if every single piece of information is going to lead to some individual arrest.

Mr. POLIQUIN. Okay. Let me drill down a little bit, if I can, Mr. El-Hindi. I only have a couple of minutes left here. Under the Bank Secrecy Act, is there liability for a financial institution to—not permit; that is not the right word—but is there a financial liability, and otherwise responsibility for a financial institution if some of the money laundering issues and other illicit activities flow through their institution? Is there liability?

Mr. EL-HINDI. Under the Bank Secrecy Act, they are required to have programs in place that enable them—

Mr. POLIQUIN. And if they don't, there is liability?

Mr. EL-HINDI. If they don't, there are liabilities.

Mr. POLIQUIN. Okay. You—

Mr. EL-HINDI. We have an Enforcement Department, and they, on occasion, will take action.

Mr. POLIQUIN. Okay. In our healthcare industry, for example, in our great country, there are instances where doctors—I don't want to be accusatory here. But there are narratives where some folks in the healthcare profession will overuse procedures—or testing, I should say, instead of procedures—because of fear of liability down the road, defensive medicine.

Do you find that might be analogous to the situation we have here where financial institutions will file these suspicious activity reports in abundance to make sure they are protecting themselves against future liability, and, therefore, it gums up your work, and we are missing opportunities to really drill down on actionable items?

Mr. EL-HINDI. This issue actually came up prior to the financial crisis, and we actually looked at the SARs to try to discern whether or not we found that data was coming into the database on a defensive basis where it had no value. And we could not see that.

The financial institutions themselves, we feel, are making good decisions about what to file and what not to file. We don't ask for perfection. We ask for them to have systems in place so that they

can meet the requirements and generally provide the information that is necessary.

And, again, as we have looked at it, we have not been able to discern this so-called defensive filing.

Mr. POLIQUIN. Mr. El-Hindi—

Mr. EL-HINDI. We are sensitive to a lot of the concerns that industry has in terms of the costs and the resources that go into it. And we continue to discuss with them better ways of making the system more efficient.

Mr. PEARCE. The gentleman's time has expired.

Mr. POLIQUIN. Thank you, Mr. Chairman.

Chairman PEARCE. The Chair now recognizes the gentleman from Arkansas, Mr. Hill, for 5 minutes.

Mr. HILL. Thank you, Mr. Chairman.

I appreciate you being here, Mr. Director. Thanks for sharing your thoughts about FinCEN.

I want to follow up on some of Mr. Emmer's questions. I have looked at a lot of material and found a number of different authorized and FTE positions. So I am just going to try to clarify that. It looks like there are 373 FTEs for FinCEN, with about 280 current positions. Is that—

Mr. EL-HINDI. I think it is closer to 340.

Mr. HILL. Okay. That is what I am saying. I have some confusing information.

And it is my understanding that there are a number of unfilled staff positions at FinCEN based on those numbers. How many exactly are unfilled, and what is the average unfilled slots for the past year or two? And is it fair to just look at FTEs versus—

Mr. EL-HINDI. I will focus on the FTEs. Currently, we have roughly 70 vacancies that we are looking to fill. Of that, roughly half are in what I will call an active recruitment process or a selection process where we are waiting for people to get through security clearances.

We have had some issues with respect to our hiring, and we are working on that. One of the things that—

Mr. HILL. What is an example of—I mean, you have security clearances. That gets backlogged.

Mr. EL-HINDI. Yes, security clearances—

Mr. HILL. Do you have a competitive pay issue at all?

Mr. EL-HINDI. Given the interest in what we do, there are instances where we lose people to the private sector.

Mr. HILL. What is the average tenure of an intel investigator for you?

Mr. EL-HINDI. I would have to get back to you on that. I don't have that.

Mr. HILL. But you do a good job of training, I would—

Mr. EL-HINDI. We do do a good job of training. And because we have a great mission, I think that we are in a position to recruit the talent that we need.

I will just say that you lose a person in about 2 weeks. The amount of time that it takes from the posting of an announcement to the selection and primarily the security clearance, the average is sometimes over a year. So that is something that we continue to work to address.

Mr. HILL. Really, for us, and the work that we do on this Terrorism Subcommittee, that is a national security problem, isn't it, that you have a year lag time in that process? As I understand it, some aspects of national security intel analysts are—have a fast-track hiring authority. Is that correct?

Mr. EL-HINDI. That is correct.

Mr. HILL. And are your slots not covered by that authority?

Mr. EL-HINDI. We are not covered by that.

Mr. HILL. Does it take legislative action to have you covered under that authority?

Mr. EL-HINDI. I would have to get back to you in terms of precisely how something like that might work.

Mr. HILL. It seems like somebody like the Secretary of the Treasury could make that happen.

So how many, roughly—is that the 70 intel analyst slots that would be covered by that—

Mr. EL-HINDI. Actually, the intel division is, I believe, almost fully staffed at this point.

Mr. HILL. Okay. If slots go unfilled and you have them authorized, which means you have the appropriated money to pay them, but they go unfilled for a year, you don't risk losing that Federal funding; it is authorized—

Mr. EL-HINDI. We have done a number of things. We work to bring on Presidential Management Fellows. We work with the Workplace Recruitment Program to try to bring people on faster.

We do have the ability to use some of that money to bring in contractors on a basis to make sure that we are able to get the work done.

Mr. HILL. If you don't mind just following up maybe with a memo on this subject that talks about authorized positions and steps you have taken to compress the hiring time and any additional authority you think the Secretary needs to have the critical national security analytic jobs be covered under that fast-track authority, that would be, I think, very helpful to the committee.

Mr. EL-HINDI. We can provide you with the information, I think.

Mr. HILL. And in the intelligence community inside the government, do people pay retention bonuses or things of that nature within the government scale to retain key employees who are sought after by the private sector?

Mr. EL-HINDI. Keep in mind that we are not part of the intelligence community.

Mr. HILL. I am throwing you in with a great group of people. You can just say thank you.

But in the law—in Federal law enforcement—I will rephrase and say, "within Federal law enforcement."

Mr. EL-HINDI. Yes. I will just say, within FinCEN, that we do have the ability to use retention bonuses.

Mr. HILL. Okay. Thank you for your time.

Thank you, Mr. Chairman.

Chairman PEARCE. The gentleman's time has expired.

The Chair now recognizes the gentlelady from Utah, Mrs. Love, for 5 minutes.

Mrs. LOVE. Thank you. Thank you, Mr. Chairman.

Thank you for being here today.

One of the concerns we hear is that financial institutions are spending so much time and money to gather information. But there is a great desire, at the same time, to make sure that the effort that is being spent to gather—is spent to gather actionable information rather than just more information. So there is a concern—and I apologize if this was covered already. We have been in and out. I just need them for my information.

There is a concern that FinCEN gets too much information and, thus, is unable to sort through it for all important indicators of crimes. Can you please address that?

Mr. EL-HINDI. It is true that we get a lot of information. And we get more information now than we did 10, 20 years ago. Actually, this is FinCEN's anniversary week. We are now 27 years old. But the capacity to digest that information and use it and disseminate it quickly has also increased over the course of time. We are in an electronic era now where the information can come in faster and can be analyzed more quickly. And we work on that.

I think that one of the things that we also try to do is make sure that the financial sector knows the many ways in which we use the information and how valuable it is.

Mrs. LOVE. Do you need to gather that much information? Are you focused on specific actionable information that you gather? Or because of the technology, do you decide to get as much as you possibly can and try and analyze it?

Mr. EL-HINDI. Keep in mind that FinCEN is a bridge between law enforcement users and the financial sector. I think one of the things that we like to point out is that law enforcement would probably want more information on basically everything that they can. As a regulator in this space, we are responsible for making sure that we are balancing burden and benefit and trying to hit the—

Mrs. LOVE. Okay. So who looks at the 55,000 reports that come in every day?

Mr. EL-HINDI. 55,000 filings come in each day. They go into the database. Within the database, they are subject to queries by 10,000 stakeholders. And essentially there are—

Mrs. LOVE. So 10,000 stakeholders are the ones who look into the—

Mr. EL-HINDI. They have the ability to use that information and access that information. But they are not—would 10,000 people be looking at every single filing that came in? That is not how it works.

Mrs. LOVE. Okay.

Mr. EL-HINDI. What we try to stress is that there is—for each filing, it has its individual value, but then collectively they have aggregate value as well. And different pieces of information filed by different financial institutions with respect to different transactions can be connected in that system.

Mrs. LOVE. Okay. Let me—

Mr. EL-HINDI. That is how we develop and understand better networks of illicit activity, by putting all of this information together.

Mrs. LOVE. Okay. Let me delve a little bit more specifically into your operations. Does FinCEN report on the commonalties found

between SARs and, namely, these common items: addresses; ID numbers; phone numbers; email addresses; IP addresses?

Mr. EL-HINDI. Commonality? I think that what—when the information is in the database, one of the things that our modernization has enabled us to do is use business rules and algorithms to help identify situations in which there may be common elements, such as you said, for example, a phone number and address that may be appearing in multiple reports coming in with respect to different transactions and particularly across different institutions. So that is a way in which those data points can be connected and we can identify network activity.

Mrs. LOVE. So, according to you, FinCEN proactively analyzes the above to find common attributes and share with law enforcement so that investigations can be initiated.

So how do the rules—how do—I am losing time. If there is extra time, I would like some extra time.

Chairman PEARCE. The gentlelady's time is extended.

Mrs. LOVE. Thank you. Oh, thank you.

How do the searches within the database work daily? What are the rules that you use when you are searching within the database daily?

Mr. EL-HINDI. I will give you an example in the terrorism context. We will identify a situation, and we will work with our team to figure out what types of terms or what types of situations might be most associated with a terrorist-type activity.

We will put that into the system, use that as a business rule, and then that will help us flag items of particular interest for further follow-up.

That is just one example of the development of a business rule.

Mrs. LOVE. So are they basically glorified Google searches? How long does—

Mr. EL-HINDI. Some types of searching of the database might be based on a simple watch list or a name type thing. Others are going to be much more complicated, weighted, multifactor analysis.

I have to apologize. I am not one of the experts with respect to the development of these types of rules. But we can certainly get back to you in terms—

Mrs. LOVE. I would like to have some details as to what the rules are. You are talking about quite a bit of information daily. I would just like to dive into that a little bit more and understand how it works.

Thank you, Mr. Chairman.

Chairman PEARCE. The gentlelady's time has expired.

The Chair now recognizes the gentleman from Ohio, Mr. Davidson, for 5 minutes.

Mr. DAVIDSON. Thank you, Mr. Chairman.

And thank you for being here and thanks for the information and the time that it takes to answer all these questions.

I am new to the committee and new to the topic as a Member of Congress anyway, but certainly right at the intersection of a lot of things where you say, "Just follow the money." And you are the folks who make that possible. So it is nice to talk with you, and I think it is an incredibly important mission.

I am particularly concerned about, how do we do that and not forget about our Bill of Rights? How do we not forget about who we are as Americans?

And one of the things that is very relevant is something in your testimony regarding Section 314(b). I am just going to read what you stated here briefly: "One issue that FinCEN frequently hears about from the financial services industry regarding information sharing is the scope of their safe harbor for information sharing under Section 314(b). The statute currently only provides safe harbor from liability for disclosing information under this section for activities that may involve terrorist activities. Activities that are predicate offenses for money laundering are not exclusively included in the provision."

So, serious activity that could lead to money laundering. When we provided the USA PATRIOT Act, we basically said: "Hey, we are going to kind of stretch the parameters of our civil liberties here because we really want to get after terrorists."

Then we said: "Well, let's go a little deeper because these things might actually lead to that."

So what kinds of safeguards are in place? Historically, that was a warrant or a subpoena. You get all this information. People are querying it. Could you go into some of the safeguards that protect civil liberties in this?

Mr. EL-HINDI. In terms of the 314, we have 314(a), which is about industry—the government sharing information back and forth between industry and government, and 314(b), which enables the institutions to share with one another.

The 314(a) authorities, as we put them in place, we have been—again, I mentioned before, we are between law enforcement and the financial sector. Part of our responsibility is to make sure that, when we are putting out requests from law enforcement for information, we do that in a responsible—

Mr. DAVIDSON. Do those requests from law enforcement come in the forms of warrants or subpoenas?

Mr. EL-HINDI. They come to us in—not in warrants or subpoenas. They come into us with respect to ongoing significant investigations.

Keep in mind that the requests come to us, and under 314(a), we are able to send that information out to financial institutions. They then say whether or not they have anything that meets—

Mr. DAVIDSON. Right now, this is a little bit like playing Go Fish and saying: "Got any transactions?"

Mr. EL-HINDI. But after that, when law enforcement reaches out to the financial institution, they then proceed with engaging with them in the normal course and—

Mr. DAVIDSON. This isn't yet personalized. In some cases, where it is just like we have this big set of data, and we just say: "Hey, do we have any transactions that look like clubs? Do you have any clubs?" To put it in Go Fish language: clubs, hearts, or diamonds. So whatever the parameter is that you are looking for, and then you go: We have these five people who have completed a transaction like that.

Or is it, instead, personalized, where you say, "I am looking for this person right here or this LLC?"

Mr. EL-HINDI. The way the requests come in to us, they are going to be much more particular. Again, the particular information we receive from law enforcement that involves their investigations is—the names are—shared with the financial institutions, and they say: Do you have transactions where these individuals or entities are involved, or do you have accounts?

If they say yes or no, then law enforcement is able to follow up with them.

It is a very efficient system. I think that one of the things that, over the course of time, because we have been able to mete out the requests and work with the financial institutions on it, it has worked very well for law enforcement. They have been—the average connection of identifying ways in which they can expand their accounts—for every request they make, they are able to identify roughly 50 transactions or accounts of interests.

Mr. DAVIDSON. Thank you for that. Most of that is (a).

But (b)—you highlight some of the categories under (a) that are the government's interaction with the bank. But then, frankly, we didn't get to all the safeguards. And we, perhaps, can schedule a briefing to go into that.

But then you go to the next layer. Now banks can share this stuff iteratively back to one another. And I don't want to dismiss that it could be effective, but I want to understand what are the civil liberty safeguards, which is something we didn't quite get to. So I would like to try to schedule time with your office to follow up.

My time has expired.

Mr. EL-HINDI. We would be happy to do that.

Chairman PEARCE. The gentleman's time has expired.

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

Mr. ZELDIN. Thank you, Mr. Chairman.

Thank you, Mr. El-Hindi, for being here today.

The issue of illicit financing and money laundering is hitting home in the most personal and tragic way in my district where we have seen ongoing violence perpetuated by MS-13 and other Central American gangs taking innocent lives and threatening the safety of our schools.

Money laundering is a key tool for these violent criminal organizations. They are tearing apart peaceful communities on Long Island and across our country. It allows them to hide their drug-trafficking revenue and transfer it illicitly across the border. That is how they buy weapons, and it fuels the growth of their dangerous criminal enterprises.

Earlier this month, we saw the senseless and tragic murders of four young men in Suffolk County, New York, which only further cemented our need to solve the gang violence problem on Long Island and nationwide. These murders have gotten the attention of both President Trump and Attorney General Sessions. Two of the victims of these murders perpetuated by MS-13 were residents of my district, and tomorrow, Attorney General Jeff Sessions will be visiting this community of Central Islip, which has been shattered by these senseless murders and other acts of transnational gang violence.

Mr. El-Hindi, we know that FinCEN, as the national experts on combating money laundering, is playing a key role to defeat threats to America's safety and security. Now more than ever we need coordination on all fronts so that our local law enforcement on our front lines can respond to this grave threat, working with other State and Federal agencies.

My first question is asking for you to speak on the effort currently to combat the threat of MS-13.

Mr. EL-HINDI. With respect to priorities that we have in FinCEN in terms of our focus, transnational organized crime, narcotrafficking, gang activity are within those priorities. When you mention Federal, State, and law enforcement working together, Federal, State, and law enforcement all have access to the data that FinCEN has, and they all have access to the support that we can provide.

To the extent that law enforcement is focused in terms of investigations and gang activity, we are there to support them and make sure that they have the best use of the information that we have.

Mr. ZELDIN. Can you walk me through how FinCEN flags suspicious activity at the local level and shares this intel with local law enforcement, especially in dealing with transnational criminal organizations like MS-13?

Mr. EL-HINDI. We have a memorandum of understanding (MOU) that allows access to our database at the Federal level, at the State level, and, in many situations, at the local level with certain municipalities.

When we have an MOU with a municipality, they have direct access to the data. In many instances, however, they can work through a State coordinator to have access to the data as well.

In terms of the products that we put out where we identify a methodology or a trend, those can go out to a wide variety of our law enforcement stakeholders.

Mr. ZELDIN. The Bank Secrecy Act puts the onus of reporting suspicious financial activity on banks. But what about violent gangs that are increasingly using apps and other technology, prepaid cards and various other nonbank instruments to launder money? How is FinCEN intercepting and monitoring those transactions and working with the local agencies on that front?

Mr. EL-HINDI. We cover more than just banks. Money transmitters are subject to our regulations. And some of the methods that you mentioned for moving money electronically might involve apps. To the extent that that activity gets into the realm of money transmission, which it often does, those financial institutions—we consider them financial institutions—are covered under the scope of our requirements. They are required to file suspicious activity reports. They are required to have programs in place to enable them to identify illicit activity and make themselves resilient to that. So that is the type of information that will go into the database.

In terms of new methods, for example, FinCEN clarified in 2013 that virtual currency exchangers, administrators of virtual currency are actually money transmitters and subject to the scope of our regulations. And we find that, by working with that industry, we are able to get valuable information to law enforcement.

Mr. ZELDIN. I appreciate that. And we certainly have law enforcement from all different levels of government and elected and community leaders. Everyone is engaged in this very important issue in Suffolk County. Again, as I mentioned, Attorney General Sessions is coming to Suffolk County tomorrow, and the President himself often talks about this issue that is in our community in Suffolk. So anything that you can possibly do to be able to assist with this effort, it is an urgent effort for my local community. And I would certainly appreciate all of your help.

I yield back.

Mr. EL-HINDI. Thank you.

Chairman PEARCE. The gentleman yields back.

The Chair now recognizes the gentleman from California, Mr. Royce, chairman of the House Foreign Affairs Committee, and a member of the full Financial Services Committee, for 5 minutes.

Mr. ROYCE. Thank you, very much, Mr. Chairman. I appreciate that.

Mr. El-Hindi, in November, the Treasury Department acknowledged to Congress that it was seeking to detail 15 FinCEN personnel to the Office of Intelligence and Analysis on a temporary basis. This committee raised concerns about the impact of the reorganization on Treasury's ability to disrupt and inhibit the financing of terrorism and other financial crimes. It was also a puzzling development in light of the fact that the Obama Administration had requested an increase in FinCEN's 2017 budget to expand the use of contractors to support FinCEN's efforts to disrupt the financing of terrorist groups, including ISIS.

So, Mr. El-Hindi, can you provide the committee with an update on the reorganization and how it is impacting your work? Is the Trump Administration supportive of or aware of the changes that their predecessor made shortly before leaving office?

Mr. EL-HINDI. I can just provide you with a little bit of context in terms of within Treasury—

Mr. ROYCE. That would be helpful.

Mr. EL-HINDI. —a focus on—I mentioned in my testimony that we are one of five components that report to the Under Secretary for Terrorism and Financial Intelligence.

There were thoughts about how we could all work better together. One aspect of that involved the idea of detailing staff from FinCEN to another component part. The status of that is it has not occurred.

Mr. ROYCE. Let me ask you another question. In its advisories, FinCEN recommends U.S. financial institutions use risk-based policies, procedures, and practices regarding jurisdictions with anti-money-laundering deficiencies. This is appropriate, but some institutions would argue that the Federal banking regulators do not themselves use a risk-based approach when they develop AML/CFT reporting requirements. To the contrary, many bankers complain that their regulators take a dragnet approach focused on burdensome and, in their view, time-consuming reporting inputs over quality outcomes.

So, Mr. El-Hindi, is it fair for FinCEN to ask financial institutions to meet a standard that the regulators do not meet? Would you agree with The Clearing House's conclusion that many, if not

most, of the resources devoted to AML/CFT by the financial sector have limited law enforcement or national security benefit? That would be one question I would ask.

And what can Congress do to refocus the Bank Secrecy Act and other legal tools on outcomes over inputs?

Mr. EL-HINDI. I will just respond to that by noting that I personally, and FinCEN generally, have talked about the fact that, along with a risk-based approach on the financial industry's part in terms of complying with our regulations, there should be a risk-based approach to regulation as well.

We have been very clear on that. And to the extent that we have to make decisions on the industries or the types of activities that we fold within the scope of our regulations, that risk-based approach to regulation is very much a part of it.

A number of things were raised in The Clearing House report that you mention. I think it is an example of a situation where industry reaches out to discuss concerns that they have with respect to how situations could be improved. FinCEN has always been eager to work with industry and discuss those ideas.

We have a forum called the Bank Secrecy Act Advisory Group where we are able to bring together law enforcement, the regulatory community, and the industry sector together with us where we can have very frank and open discussions about what is working, and what is not working. A lot of the issues that are raised in the paper that you mention are things that we discuss and are working on within that context. But we have always been eager to work with industry and law enforcement to make sure that we are on the right track and that we are doing the right things.

That is why we have—I continue to say that we are a bridge between both worlds. To the extent that neither is completely satisfied with the results that we sometimes come up with, it probably is an indication that we are doing the right thing.

Mr. ROYCE. Mr. El-Hindi, thank you very much.

I yield back.

Chairman PEARCE. The gentleman yields back.

Mr. El-Hindi, you have been very gracious with your time. If you could spare just a couple more minutes.

You are part of a group of about 150 FIUs worldwide. Of those, which would you estimate has probably the best information technology sharing?

Mr. EL-HINDI. I am not in a position right now to comment on particular jurisdictions. We have strong relationships with many of our FIU partners, and there are other relationships that we would like to improve. At the same time, there are some of our FIUs that are in great shape in terms of their ability to do things and others that would need to improve.

In some of the rulemaking that we have discussed, if you go through past FinCEN records, you can see a close involvement that we have with our Canadian counterparts, our Australian counterparts, and other counterparts as well. But I am not in a position to comment on the strengths—

Chairman PEARCE. If you could reach out and grab someone's technology and put it into FinCEN, whose would that be? Do you have an opinion about that?

Mr. EL-HINDI. I am not in a position to comment on that right now. I would just say that one of the great things about being an FIU and having a forum that we can compare the tools that we have and the authorities that we have is that it does create opportunities for us to think along those lines. And that happens.

I mentioned virtual currency earlier today. When we came out with our interpretation of virtual currency, our FIU counterparts from other jurisdictions were on the phone, and we were comparing notes. And in terms of how we approach that situation, the same could be true with respect to the technology as well. And we do have workshops with them in which we can compare ideas.

Chairman PEARCE. And if you were going to take a guess—again, these are highly speculative things—how many of the 150 would like to take ours and implement? I am still trying to drive—

Mr. EL-HINDI. How many of them—

Chairman PEARCE. Would like to use our technology instead of the one they have? Half? Three quarters? All of them?

Mr. EL-HINDI. I would—given—

Chairman PEARCE. I am just trying to figure out kind of where we stand in the world as far as our expertise and our capabilities from the IT point, not the human capacity.

Mr. EL-HINDI. I think that we are up there. And others are up there as well.

Chairman PEARCE. Okay. So we are in the top 10 percent or so? Top 30 percent?

Mr. EL-HINDI. I will just say we are up there, and others are up there as well.

Chairman PEARCE. You have been very gracious. We appreciate everything.

I would like to thank you for your testimony today and for answering all of our questions.

The Chair notes that some Members may have additional questions for this witness, 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 this witness and to place his 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 4:35 p.m., the hearing was adjourned.]

A P P E N D I X

April 27, 2017

STATEMENT OF

JAMAL EL-HINDI, ACTING DIRECTOR
FINANCIAL CRIMES ENFORCEMENT NETWORK
UNITED STATES DEPARTMENT OF THE TREASURY

BEFORE THE

UNITED STATES HOUSE OF REPRESENTATIVES
COMMITTEE ON FINANCIAL SERVICES
SUBCOMMITTEE ON TERRORISM AND ILLICIT FINANCE

APRIL 27, 2017

NOT FOR PUBLICATION UNTIL RELEASED BY THE HOUSE COMMITTEE ON FINANCIAL SERVICES, SUBCOMMITTEE ON TERRORISM AND ILLICIT FINANCE

Chairman Pearce, Vice Chairman Pittenger, Ranking Member Perlmutter, and distinguished members of the Subcommittee, thank you for inviting me to appear before you today to discuss the role of the Financial Crimes Enforcement Network (FinCEN) in collecting, analyzing, and disseminating Bank Secrecy Act (BSA) data, and to share with you some new and evolving money laundering and terrorist financing challenges. I appreciate the Subcommittee's interest in these important issues and your continued support of our efforts.

FinCEN – a bureau of the U.S. Department of the Treasury within the Office of Terrorism and Financial Intelligence (TFI) – is charged with safeguarding the financial system from illicit use, combating money laundering, and promoting national security through the collection, analysis, and dissemination of BSA information and strategic use of BSA authorities. We strive for the responsible use of financial information for greater security and integrity of the U.S. financial system. FinCEN works to achieve its mission through a broad range of interrelated strategies, including:

- Implementing, administering, and enforcing the BSA – the United States' primary anti-money laundering and countering the financing of terrorism (AML/CFT) regulatory regime;
- Supporting law enforcement, intelligence and regulatory agencies through the sharing and analysis of BSA information;
- Serving as the Financial Intelligence Unit (FIU) for the United States; and
- Building international cooperation and technical expertise among the global network of FIUs.

To accomplish these activities, FinCEN employs a team of dedicated employees with a broad range of expertise in illicit finance, financial intelligence, the financial industry, the AML/CFT regulatory regime, technology, and enforcement. FinCEN's ability to work closely with regulatory, law enforcement, international, and industry partners promotes consistency across our regulatory regime and protects the U.S. financial system.

Collection, Analysis and Dissemination of Bank Secrecy Act Data

The BSA is the primary federal AML law. It requires a broad range of U.S. financial institutions to establish AML programs, maintain records, and provide reports to FinCEN. The majority of BSA data FinCEN collects comes from two reporting streams: Currency Transaction Reports (CTRs) and Suspicious Activity Reports (SARs). Financial institutions[1] must file CTRs with FinCEN for cash transactions totaling more than $10,000 and file SARs to report suspicious transactions. Both the objective reporting in CTRs and the subjective reporting in SARs are critically important; they provide a wealth of potentially useful information to FinCEN and other agencies working to detect and prevent money laundering, other financial crimes, and terrorism.

Thanks to funding from Congress, FinCEN successfully completed an Information Technology (IT) modernization program in 2014, updating the process of collecting, analyzing and disseminating BSA data. FinCEN accomplished five significant goals through this program: FinCEN 1) assumed responsibility for maintaining BSA data in a FinCEN-based system; 2) shifted from paper filings of BSA reports to the electronic filing of BSA reports; 3) developed a new IT system for approved law enforcement and regulatory partners to access BSA data; 4) strengthened IT security through implementation of two-factor authentication and other mechanisms; and 5) developed foundational advanced analytics capabilities to enhance FinCEN's ability to exploit BSA data.

FinCEN receives an average of roughly 55,000 new financial institution filings each day. These filings come from more than 80,000 financial institutions and 500,000 individual foreign bank account holders through FinCEN's modernized E-filing system. FinCEN maintains over 200 million of these BSA filings in our database. FinCEN makes this information available to more than 10,000 law enforcement and other government users through a search tool designed to meet their specialized needs, known as FinCEN Query. These users, in turn, perform approximately 30,000 daily searches of the data. E-filing has streamlined the reporting process for financial institutions and individual filers and significantly improved users' ability to exploit BSA data by making it more accessible and searchable.

---

[1] Examples of institutions that file SARs and/or CTRs include: banks and credit unions, money remitters, check cashers, virtual currency exchangers, casinos and card clubs, and dealers in foreign exchange.

The protection of the sensitive information we receive is also a critical part of our mission. FinCEN safeguards BSA data through a continual process of reviewing IT security measures and processes in place, adjusting to current and emerging risks, and ensuring that security is a consistent requirement considered throughout the lifecycle of each system. FinCEN systems are accredited to High Federal Information Security Management Act (FISMA) levels and employ strong security mechanisms such as two-factor authentication, encryption, and activity monitoring to protect BSA data. FinCEN works with the Department of the Treasury and the Department of Homeland Security cyber security organizations for security operations and mitigation activities.

The FinCEN Financial Intelligence Cycle

FinCEN delivers BSA information and related analysis to law enforcement, regulatory, foreign, and private sector partners following an intelligence cycle methodology. This cycle involves the collection, processing, exploitation, and dissemination of BSA-derived financial intelligence, and the direction of future BSA collection efforts

In terms of collection, the first stage of the financial intelligence cycle, FinCEN has the ability to collect more than routinely filed BSA data. FinCEN can proactively target certain financial intelligence for collection using a variety of authorities and special measures. Some of these targeted financial intelligence collection tools include:

- Section 314(a) of the USA PATRIOT Act, which authorizes FinCEN to share law enforcement and regulatory information with financial institutions on individuals, entities, and organizations reasonably suspected of engaging in terrorist acts or money laundering activities, in order to collect related financial intelligence.

- Geographic Targeting Order (GTO) authority, which enables FinCEN to impose additional recordkeeping or reporting requirements on domestic financial institutions or other businesses in a specific geographic area identified in the order for 180 days.

- Foreign Financial Agency authority, which enables FinCEN to impose additional reporting requirements on U.S. financial institutions about their transactions with designated foreign financial entities.

- Demand Letters, which are requests by FinCEN for records relating to international funds transfers of $3,000 or more. The scope of the requested information can vary depending on the specific circumstances of the request.

Processing is the second stage of the financial intelligence cycle. With approximately 55,000 filings per day, advanced technology solutions are needed to review, analyze, and quickly disseminate time-sensitive information. To manage a data collection of this size and to rapidly identify nodes and patterns of potentially illicit activity for further action, FinCEN employs a number of advanced analytic approaches.

To combat our most significant money laundering and terrorist financing threats, FinCEN employs automated business rules to screen filings on a daily basis and identify reports that merit further review by analysts. The rules range in complexity from traditional "watch list" rules designed to identify known illicit actors to complex multi-variable weighted rule sets capable of identifying potential illicit activity.

These algorithms search the reporting for key terms, entities, and typologies of interest daily, across six priority areas: transnational security threats; cybercrime; transnational organized crime; significant fraud; compromised financial institutions or third party money laundering; and data quality, benchmarking, and anomaly detection. The business rules produce approximately 5,000 rule findings per month, pointing FinCEN analysts to specific filings for hands-on review and focusing their efforts on the filings most likely to be key to defending against priority threats. This produces an important stream of timely financial intelligence for FinCEN analysts and external stakeholders.

FinCEN analysts work, often with input from investigators internal and external to FinCEN, to design models and analytic techniques that identify newly trending illicit typologies; monitor responses to FinCEN advisories, geographic targeting orders, and other regulatory actions; locate potential data quality issues; and flag matters that potentially exhibit behavior patterns indicative of significant money laundering activity.

For the analysis and dissemination stages of FinCEN's financial intelligence cycle, we have consolidated analytic capabilities and expanded the scope of our work to create products that

address critical priority threats for our stakeholders, including the financial industry. FinCEN combines BSA data with additional information, commercial data sources, and other open source material to develop proactive targets and strategic assessments of money laundering trends and vulnerabilities for dissemination to our partners, both domestic and international.

Lastly, the financial intelligence cycle helps inform future planning and direction. Once threats and vulnerabilities have been identified, FinCEN can adjust the regulatory framework protecting the U.S. financial system. FinCEN uses its regulatory rulemaking authority to, among other things, define the reporting that financial institutions and others must provide. FinCEN also develops advisories to inform industry about money laundering and terrorist financing threats, including the red flag indicators in their data that might be indicative of suspicious activity. These rulemaking activities and advisories expand and/or improve the information that FinCEN collects. The dovetailing of this phase with the collection phase confirms the iterative and cyclical nature of our financial intelligence activities.

Information Sharing

Financial intelligence is most effective when information flows in both directions between the public and private sectors. FinCEN serves as a communication point between financial institutions and law enforcement, regulatory, and international colleagues. Providing information to the financial industry, based on our analysis of their own reporting, is a force-multiplier.

One of the tools FinCEN uses to report suspicious behaviors possibly related to money laundering and terrorist financing threats to industry – and thus generate additional reporting that may address these suspicions – is our Financial Institution Advisory Program. FinCEN can issue public and non-public advisories to alert financial institutions of specific illicit finance risks. Advisories often contain illicit activity typologies, red flags to facilitate monitoring, and guidance on complying with FinCEN regulations to address threats and vulnerabilities. Financial institutions may use this information to enhance their AML monitoring systems for more valuable suspicious activity reporting.

The threat posed by al-Qaida, the Islamic State of Iraq and Syria (ISIS), their respective branches and affiliates, and associated foreign terrorist fighters is a key focus for FinCEN and TFI as a whole. The reporting by financial institutions is an essential component in identifying foreign terrorist fighters, financial and logistical facilitators, and their methods of moving funds. In May 2015, FinCEN issued a non-public advisory related to ISIS financing. Following the publication of the advisory, financial institutions used FinCEN's 24/7 reporting hotline to notify FinCEN of possible terrorist financing activity. This included amendments to previously reported suspicious activity where the filer had not realized at the time a potential ISIS connection, as well as new reporting of suspicious activity specifically referencing the advisory. It is important to note that both large and small financial institutions made reports, which demonstrates the utility of our collection process and the seriousness with which the financial industry takes its reporting obligations.

In December 2015, FinCEN issued another non-public advisory to U.S. financial institutions, providing some "red flag" indicators to help financial institutions identify and report financial transactions that may be associated with foreign terrorist fighters who support ISIS, al-Qaida, and their affiliates in Iraq and Syria. The advisory resulted in new terrorist financing-related SARs, the amending of past SARs to indicate possible terrorist financing, and more terrorist financing tips to FinCEN's 24/7 reporting hotline.

The suspicious activity that financial institutions have identified based in part on these advisories, coupled with their own analyses, generates extremely valuable financial intelligence that FinCEN shares with our law enforcement partners.

Another useful tool for sharing information is Section 314 of the USA PATRIOT Act. FinCEN has placed significant emphasis on our public-private partnerships and on information sharing under Section 314 of the USA PATRIOT Act. Section 314(a) essentially involves sharing of information between financial institutions and government, while Section 314(b) involves sharing of information among financial institutions themselves.

FinCEN has a well-established domestic and international program implementing Section 314(a), which allows FinCEN to request certain information from financial institutions related to money laundering and terrorist financing. This authority is used to canvass the financial system

to identify accounts or transactions at the request of law enforcement. The 314(a) process has proven to be an effective tool in many law enforcement investigations with 95 percent of the 314(a) requests contributing to arrests or indictments.

Section 314(b) allows financial institutions to voluntarily share information with one another under a safe harbor that offers protections from liability in order to better identify and report potential money laundering or terrorist activities. While information sharing under the 314(b) program is voluntary, it can help financial institutions enhance compliance with their AML/CFT obligations, most notably with respect to:

- Gathering additional information on customers or transactions potentially related to money laundering or terrorist financing, including previously unknown accounts, activities, and/or associated entities or individuals;
- Shedding more light upon overall financial trails, especially if they are complex and appear to be layered amongst numerous financial institutions, entities, and jurisdictions;
- Building a more comprehensive and accurate picture of a customer's activities where potential money laundering or terrorist financing is suspected, allowing for more precise decision-making in due diligence and transaction monitoring;
- Alerting other participating financial institutions to customers whose suspicious activities those institutions may not have been previously aware;
- Facilitating the filing of more comprehensive SARs than would otherwise be filed in the absence of 314(b) information sharing;
- Identifying and aiding in the detection of money laundering and terrorist financing methods and schemes; and
- Facilitating efficient SAR reporting decisions by enabling financial institutions to obtain a more complete picture of activity through the voluntary information sharing process.

One issue frequently noted by industry regarding information sharing is the scope of their safe harbor for information sharing under Section 314(b). The statute currently provides a safe

harbor from liability for disclosing information under Section 314(b) for activities that may involve terrorist actions or money laundering activities. Activities that are the predicates for money laundering, like fraud, drug trafficking, cybercrimes, and others, are not explicitly included in the safe harbor. FinCEN issued guidance on the expansive scope of permissible information sharing covered by Section 314(b) safe harbor in 2009. .

In addition to close collaboration with domestic partners, FinCEN works to establish and strengthen mechanisms for the exchange of information globally, and to engage with, encourage, and support international partners in taking necessary steps to construct regimes to combat money laundering, terrorist financing, and other financial crimes. FinCEN responds to requests from FIUs that are members of the Egmont Group and acts as a conduit for requests from domestic law enforcement to foreign FIUs. We also proactively share information with this global network of FIUs. By leveraging the network of more than 150 FIUs globally to exchange valuable financial intelligence, we are able to work together to combat terrorist financing and money laundering threats across jurisdictional boundaries.

New and Evolving Money Laundering and Terrorist Financing Challenges

To effectively counter money laundering and the financing of terrorism, we must understand the threats, risks, and vulnerabilities posed to the U.S. and global financial systems by the broad array of illicit financial activity. We must keep a constant watch for new and emerging challenges and threats and be more creative in using our existing authorities and exploring new tools that will aid in the fight against money laundering and terrorist financing. I would like to highlight three focus areas: real estate, virtual currency, and cybersecurity.

Real Estate

FinCEN is working actively to address money laundering and terrorist financing risks in the real estate sector. FinCEN has had longstanding concerns that "all-cash" real estate transactions, i.e., those without bank financing, which are largely outside the scope of most existing AML requirements, may present money laundering vulnerabilities, particularly where a purchaser uses a shell company to conceal the true buyer. FinCEN issued Geographic Targeting Orders in January 2016 covering the Borough of Manhattan in New York, and Miami, Florida, to further

evaluate the extent of this potential money laundering vulnerability. These GTOs required certain U.S. title insurance companies to record and report the beneficial ownership information of legal entities making "all-cash" purchases of high-value residential real estate in these two geographic areas. In July 2016, FinCEN renewed the GTOs and extended coverage to additional areas in New York City, South Florida, California, and Texas. The GTOs, including the extended coverage, were renewed in February 2017.

At the time of the most recent renewal, approximately 30 percent of the real estate transactions reported under the GTOs involved a beneficial owner or purchaser representative that also had previously been the subject of a SAR. In other words, the beneficial owners or purchaser representatives in a significant portion of transactions reported under the GTO had been previously connected to suspicious activity. As a result of the attention generated by the GTOs, we have seen additional SAR filings related to potential money laundering involving real estate. In total, these SARs, along with the information generated by the GTOs, are advancing law enforcement's ability to identify potentially illicit activity and are helping inform FinCEN's broader AML approach towards the real estate sector.

While the GTO authority is a useful tool to obtain additional targeted information to inform regulatory and law enforcement efforts, there are significant limitations on the types of information that can be collected using a GTO. Under the authorizing statute, such orders may only be used to collect information on transactions involving currency or similar monetary instruments. Transactions that do not involve such instruments, such as wire transfers, may not be covered. When FinCEN works to gather information on transactions that are conducted through means other than currency or monetary instruments, as is the case with real estate transactions where the use of wires is common in many locations, the data we can gather is more limited.

Virtual Currency

The global financial industry is experiencing a period of technological innovation and growth that also creates new vulnerabilities that FinCEN and our partners must understand to prevent gaps in regulation and information collection on terrorist financing and other illicit activity.

For instance, in the virtual currency space, FinCEN has been at the forefront of engagement that balances these interests. In 2013, FinCEN released interpretive guidance on virtual currencies to provide regulatory consistency to a nascent area of the financial industry that implicated significant AML/CFT equities.

Any financial institution, payment system, or medium of exchange has the potential to be exploited for money laundering or terrorist financing. Virtual currency is not different in this regard. As with all parts of the financial system, FinCEN seeks to understand the specific attributes that make virtual currency vulnerable to illicit use, and then employ a smart regulatory approach and encourage industry to develop mitigating features in its products. Financial institutions that deal in virtual currency must put effective AML/CFT controls in place to protect themselves from illicit actors that attempt to exploit identified vulnerabilities. To that end, in May 2015, in coordination with federal law enforcement partners, FinCEN assessed the first civil monetary penalty against a virtual currency exchanger, Ripple Labs Inc., for failure to register with FinCEN as a money services business and implement and maintain an adequate AML program designed to protect its production from use by money launderers or terrorist financiers.

Cybersecurity

The size, reach, speed, and accessibility of the U.S. financial system make financial institutions attractive targets to traditional criminals, cybercriminals, terrorists, and state actors. These actors target financial institutions' websites, systems, and employees to steal customer and commercial credentials and proprietary information; defraud financial institutions and their customers; or disrupt business functions. Financial institutions play an important role in safeguarding customers and the financial system from these threats through timely and thorough reporting of cyber-events and cyber-related information in SARs. In 2016, FinCEN received more than 60,000 cyber-related SARs describing a range of cyber-enabled financial crimes.

Improved financial transparency and increased information sharing can help address the challenges posed in the cybersecurity domain. FinCEN issued an advisory in October 2016 to raise awareness among financial institutions about the intersection between cyber and AML/CFT issues. The advisory clarifies how financial institutions should approach cyber issues as they relate to SAR obligations. It also encourages coordination between AML and cybersecurity staff

to mitigate risks. In addition to the advisory, FinCEN published answers to Frequently Asked Questions concerning the filing of related SARs. We are also actively sharing indicators of suspicious cyber activity with industry, publishing more than 18,000 indicators since the launch of the program in late 2016.

In September 2016, FinCEN issued an advisory on e-mail compromise fraud schemes. It describes a variety of e-mail fraud schemes and details red flags – developed in consultation with law enforcement, including the Federal Bureau of Investigation and the U.S. Secret Service – that financial institutions may use to identify and help prevent such frauds. The schemes focus on using compromised e-mail accounts to mislead financial institutions and their customers into conducting unauthorized wire transfers. In addition to alerting industry to the types of schemes to look out for, the advisory encourages rapid communication to law enforcement when a fraudulent transaction occurs. Where U.S. businesses or financial institutions quickly alert law enforcement, FinCEN often has been able to work with its foreign counterparts to assist in the return of funds sent overseas by business email compromise schemes. Over the past two years, with respect to the illicit overseas transfer of roughly $491 million brought to our attention, we have been able to help in the return of over $275 million.

FinCEN and law enforcement agencies regularly use BSA data reported by financial institutions to initiate investigations, identify and track criminals, and disrupt and dismantle criminal networks. FinCEN strives to share actionable information with industry to help financial institutions identify and report on cyber-related suspicious activity. FinCEN will continue to share information about such threats regularly with our partners in both government and industry.

Conclusion

The current AML/CFT landscape is complex, dynamic, and requires ongoing adaptation by FinCEN and our many partners. As we continue to adjust to ever-evolving threats, we will continue to use the tools at our disposal to collect financial intelligence information, analyze it, and deploy it in support of FinCEN's mission to safeguard the financial system from illicit use, combat money laundering and terrorist financing, and promote national security.

Chairman Pearce, Vice Chairman Pittenger, Ranking Member Perlmutter, and members of the Subcommittee, thank you again for the opportunity to testify today and for your continued support of FinCEN's important mission. I look forward to your questions.

Department of the Treasury
Financial Crimes Enforcement Network

Guidance

FIN-2014-G001
Issued: February 14, 2014
Subject: BSA Expectations Regarding Marijuana-Related Businesses

The Financial Crimes Enforcement Network ("FinCEN") is issuing guidance to clarify Bank Secrecy Act ("BSA") expectations for financial institutions seeking to provide services to marijuana-related businesses. FinCEN is issuing this guidance in light of recent state initiatives to legalize certain marijuana-related activity and related guidance by the U.S. Department of Justice.("DOJ") concerning marijuana-related enforcement priorities. This FinCEN guidance clarifies how financial institutions can provide services to marijuana-related businesses consistent with their BSA obligations, and aligns the information provided by financial institutions in BSA reports with federal and state law enforcement priorities. This FinCEN guidance should enhance the availability of financial services for, and the financial transparency of, marijuana-related businesses.

Marijuana Laws and Law Enforcement Priorities

The Controlled Substances Act ("CSA") makes it illegal under federal law to manufacture, distribute, or dispense marijuana.[1] Many states impose and enforce similar prohibitions. Notwithstanding the federal ban, as of the date of this guidance, 20 states and the District of Columbia have legalized certain marijuana-related activity. In light of these developments, U.S. Department of Justice Deputy Attorney General James M. Cole issued a memorandum (the "Cole Memo") to all United States Attorneys providing updated guidance to federal prosecutors concerning marijuana enforcement under the CSA.[2] The Cole Memo guidance applies to all of DOJ's federal enforcement activity, including civil enforcement and criminal investigations and prosecutions, concerning marijuana in all states.

The Cole Memo reiterates Congress's determination that marijuana is a dangerous drug and that the illegal distribution and sale of marijuana is a serious crime that provides a significant source of revenue to large-scale criminal enterprises, gangs, and cartels. The Cole Memo notes that DOJ is committed to enforcement of the CSA consistent with those determinations. It also notes that DOJ is committed to using its investigative and prosecutorial resources to address the most

[1] Controlled Substances Act, 21 U.S.C. § 801, *et seq.*
[2] James M. Cole, Deputy Attorney General, U.S. Department of Justice, *Memorandum for All United States Attorneys: Guidance Regarding Marijuana Enforcement* (August 29, 2013), *available at* http://www.justice.gov/iso/opa/resources/3052013829132756857467.pdf.

significant threats in the most effective, consistent, and rational way. In furtherance of those objectives, the Cole Memo provides guidance to DOJ attorneys and law enforcement to focus their enforcement resources on persons or organizations whose conduct interferes with any one or more of the following important priorities (the "Cole Memo priorities"):[3]

- Preventing the distribution of marijuana to minors;
- Preventing revenue from the sale of marijuana from going to criminal enterprises, gangs, and cartels;
- Preventing the diversion of marijuana from states where it is legal under state law in some form to other states;
- Preventing state-authorized marijuana activity from being used as a cover or pretext for the trafficking of other illegal drugs or other illegal activity;
- Preventing violence and the use of firearms in the cultivation and distribution of marijuana;
- Preventing drugged driving and the exacerbation of other adverse public health consequences associated with marijuana use;
- Preventing the growing of marijuana on public lands and the attendant public safety and environmental dangers posed by marijuana production on public lands; and
- Preventing marijuana possession or use on federal property.

Concurrently with this FinCEN guidance, Deputy Attorney General Cole is issuing supplemental guidance directing that prosecutors also consider these enforcement priorities with respect to federal money laundering, unlicensed money transmitter, and BSA offenses predicated on marijuana-related violations of the CSA.[4]

Providing Financial Services to Marijuana-Related Businesses

This FinCEN guidance clarifies how financial institutions can provide services to marijuana-related businesses consistent with their BSA obligations. In general, the decision to open, close, or refuse any particular account or relationship should be made by each financial institution based on a number of factors specific to that institution. These factors may include its particular business objectives, an evaluation of the risks associated with offering a particular product or service, and its capacity to manage those risks effectively. Thorough customer due diligence is a critical aspect of making this assessment.

In assessing the risk of providing services to a marijuana-related business, a financial institution should conduct customer due diligence that includes: (i) verifying with the appropriate state authorities whether the business is duly licensed and registered; (ii) reviewing the license application (and related documentation) submitted by the business for obtaining a state license to operate its marijuana-related business; (iii) requesting from state licensing and enforcement authorities available information about the business and related parties; (iv) developing an understanding of the normal and expected activity for the business, including the types of

[3] The Cole Memo notes that these enforcement priorities are listed in general terms; each encompasses a variety of conduct that may merit civil or criminal enforcement of the CSA.
[4] James M. Cole, Deputy Attorney General, U.S. Department of Justice, *Memorandum for All United States Attorneys: Guidance Regarding Marijuana Related Financial Crimes* (February 14, 2014).

products to be sold and the type of customers to be served (e.g., medical versus recreational customers); (v) ongoing monitoring of publicly available sources for adverse information about the business and related parties; (vi) ongoing monitoring for suspicious activity, including for any of the red flags described in this guidance; and (vii) refreshing information obtained as part of customer due diligence on a periodic basis and commensurate with the risk. With respect to information regarding state licensure obtained in connection with such customer due diligence, a financial institution may reasonably rely on the accuracy of information provided by state licensing authorities, where states make such information available.

As part of its customer due diligence, a financial institution should consider whether a marijuana-related business implicates one of the Cole Memo priorities or violates state law. This is a particularly important factor for a financial institution to consider when assessing the risk of providing financial services to a marijuana-related business. Considering this factor also enables the financial institution to provide information in BSA reports pertinent to law enforcement's priorities. A financial institution that decides to provide financial services to a marijuana-related business would be required to file suspicious activity reports ("SARs") as described below.

Filing Suspicious Activity Reports on Marijuana-Related Businesses

The obligation to file a SAR is unaffected by any state law that legalizes marijuana-related activity. A financial institution is required to file a SAR if, consistent with FinCEN regulations, the financial institution knows, suspects, or has reason to suspect that a transaction conducted or attempted by, at, or through the financial institution: (i) involves funds derived from illegal activity or is an attempt to disguise funds derived from illegal activity; (ii) is designed to evade regulations promulgated under the BSA, or (iii) lacks a business or apparent lawful purpose.[5] Because federal law prohibits the distribution and sale of marijuana, financial transactions involving a marijuana-related business would generally involve funds derived from illegal activity. Therefore, a financial institution is required to file a SAR on activity involving a marijuana-related business (including those duly licensed under state law), in accordance with this guidance and FinCEN's suspicious activity reporting requirements and related thresholds.

One of the BSA's purposes is to require financial institutions to file reports that are highly useful in criminal investigations and proceedings. The guidance below furthers this objective by assisting financial institutions in determining how to file a SAR that facilitates law enforcement's access to information pertinent to a priority.

"Marijuana Limited" SAR Filings

A financial institution providing financial services to a marijuana-related business that it reasonably believes, based on its customer due diligence, does not implicate one of the Cole Memo priorities or violate state law should file a "Marijuana Limited" SAR. The content of this

[5] *See, e.g.*, 31 CFR § 1020.320. Financial institutions shall file with FinCEN, to the extent and in the manner required, a report of any suspicious transaction relevant to a possible violation of law or regulation. A financial institution may also file with FinCEN a SAR with respect to any suspicious transaction that it believes is relevant to the possible violation of any law or regulation but whose reporting is not required by FinCEN regulations.

SAR should be limited to the following information: (i) identifying information of the subject and related parties; (ii) addresses of the subject and related parties; (iii) the fact that the filing institution is filing the SAR solely because the subject is engaged in a marijuana-related business; and (iv) the fact that no additional suspicious activity has been identified. Financial institutions should use the term "MARIJUANA LIMITED" in the narrative section.

A financial institution should follow FinCEN's existing guidance on the timing of filing continuing activity reports for the same activity initially reported on a "Marijuana Limited" SAR.[6] The continuing activity report may contain the same limited content as the initial SAR, plus details about the amount of deposits, withdrawals, and transfers in the account since the last SAR. However, if, in the course of conducting customer due diligence (including ongoing monitoring for red flags), the financial institution detects changes in activity that potentially implicate one of the Cole Memo priorities or violate state law, the financial institution should file a "Marijuana Priority" SAR.

"Marijuana Priority" SAR Filings

A financial institution filing a SAR on a marijuana-related business that it reasonably believes, based on its customer due diligence, implicates one of the Cole Memo priorities or violates state law should file a "Marijuana Priority" SAR. The content of this SAR should include comprehensive detail in accordance with existing regulations and guidance. Details particularly relevant to law enforcement in this context include: (i) identifying information of the subject and related parties; (ii) addresses of the subject and related parties; (iii) details regarding the enforcement priorities the financial institution believes have been implicated; and (iv) dates, amounts, and other relevant details of financial transactions involved in the suspicious activity. Financial institutions should use the term "MARIJUANA PRIORITY" in the narrative section to help law enforcement distinguish these SARs.[7]

"Marijuana Termination" SAR Filings

If a financial institution deems it necessary to terminate a relationship with a marijuana-related business in order to maintain an effective anti-money laundering compliance program, it should

---

[6] Frequently Asked Questions Regarding the FinCEN Suspicious Activity Report (Question #16), *available at:* http://fincen.gov/whatsnew/html/sar_faqs.html (providing guidance on the filing timeframe for submitting a continuing activity report).

[7] FinCEN recognizes that a financial institution filing a SAR on a marijuana-related business may not always be well-positioned to determine whether the business implicates one of the Cole Memo priorities or violates state law, and thus which terms would be most appropriate to include (i.e., "Marijuana Limited" or "Marijuana Priority"). For example, a financial institution could be providing services to another domestic financial institution that, in turn, provides financial services to a marijuana-related business. Similarly, a financial institution could be providing services to a non-financial customer that provides goods or services to a marijuana-related business (e.g., a commercial landlord that leases property to a marijuana-related business). In such circumstances where services are being provided indirectly, the financial institution may file SARs based on existing regulations and guidance without distinguishing between "Marijuana Limited" and "Marijuana Priority." Whether the financial institution decides to provide indirect services to a marijuana-related business is a risk-based decision that depends on a number of factors specific to that institution and the relevant circumstances. In making this decision, the institution should consider the Cole Memo priorities, to the extent applicable.

file a SAR and note in the narrative the basis for the termination. Financial institutions should use the term "MARIJUANA TERMINATION" in the narrative section. To the extent the financial institution becomes aware that the marijuana-related business seeks to move to a second financial institution, FinCEN urges the first institution to use Section 314(b) voluntary information sharing (if it qualifies) to alert the second financial institution of potential illegal activity. See *Section 314(b) Fact Sheet* for more information.[8]

Red Flags to Distinguish Priority SARs

The following red flags indicate that a marijuana-related business may be engaged in activity that implicates one of the Cole Memo priorities or violates state law. These red flags indicate only possible signs of such activity, and also do not constitute an exhaustive list. It is thus important to view any red flag(s) in the context of other indicators and facts, such as the financial institution's knowledge about the underlying parties obtained through its customer due diligence. Further, the presence of any of these red flags in a given transaction or business arrangement may indicate a need for additional due diligence, which could include seeking information from other involved financial institutions under Section 314(b). These red flags are based primarily upon schemes and typologies described in SARs or identified by our law enforcement and regulatory partners, and may be updated in future guidance.

- A customer appears to be using a state-licensed marijuana-related business as a front or pretext to launder money derived from other criminal activity (i.e., not related to marijuana) or derived from marijuana-related activity not permitted under state law. Relevant indicia could include:
    - The business receives substantially more revenue than may reasonably be expected given the relevant limitations imposed by the state in which it operates.
    - The business receives substantially more revenue than its local competitors or than might be expected given the population demographics.
    - The business is depositing more cash than is commensurate with the amount of marijuana-related revenue it is reporting for federal and state tax purposes.
    - The business is unable to demonstrate that its revenue is derived exclusively from the sale of marijuana in compliance with state law, as opposed to revenue derived from (i) the sale of other illicit drugs, (ii) the sale of marijuana not in compliance with state law, or (iii) other illegal activity.
    - The business makes cash deposits or withdrawals over a short period of time that are excessive relative to local competitors or the expected activity of the business.

[8] Information Sharing Between Financial Institutions: Section 314(b) Fact Sheet, *available at: http://fincen.gov/statutes_regs/patriot/pdf/314bfactsheet.pdf.*

- Deposits apparently structured to avoid Currency Transaction Report ("CTR") requirements.
- Rapid movement of funds, such as cash deposits followed by immediate cash withdrawals.
- Deposits by third parties with no apparent connection to the accountholder.
- Excessive commingling of funds with the personal account of the business's owner(s) or manager(s), or with accounts of seemingly unrelated businesses.
- Individuals conducting transactions for the business appear to be acting on behalf of other, undisclosed parties of interest.
- Financial statements provided by the business to the financial institution are inconsistent with actual account activity.
- A surge in activity by third parties offering goods or services to marijuana-related businesses, such as equipment suppliers or shipping servicers.

- The business is unable to produce satisfactory documentation or evidence to demonstrate that it is duly licensed and operating consistently with state law.
- The business is unable to demonstrate the legitimate source of significant outside investments.
- A customer seeks to conceal or disguise involvement in marijuana-related business activity. For example, the customer may be using a business with a non-descript name (e.g., a "consulting," "holding," or "management" company) that purports to engage in commercial activity unrelated to marijuana, but is depositing cash that smells like marijuana.
- Review of publicly available sources and databases about the business, its owner(s), manager(s), or other related parties, reveal negative information, such as a criminal record, involvement in the illegal purchase or sale of drugs, violence, or other potential connections to illicit activity.
- The business, its owner(s), manager(s), or other related parties are, or have been, subject to an enforcement action by the state or local authorities responsible for administering or enforcing marijuana-related laws or regulations.
- A marijuana-related business engages in international or interstate activity, including by receiving cash deposits from locations outside the state in which the business operates, making or receiving frequent or large interstate transfers, or otherwise transacting with persons or entities located in different states or countries.

- The owner(s) or manager(s) of a marijuana-related business reside outside the state in which the business is located.

- A marijuana-related business is located on federal property or the marijuana sold by the business was grown on federal property.

- A marijuana-related business's proximity to a school is not compliant with state law.

- A marijuana-related business purporting to be a "non-profit" is engaged in commercial activity inconsistent with that classification, or is making excessive payments to its manager(s) or employee(s).

Currency Transaction Reports and Form 8300's

Financial institutions and other persons subject to FinCEN's regulations must report currency transactions in connection with marijuana-related businesses the same as they would in any other context, consistent with existing regulations and with the same thresholds that apply. For example, banks and money services businesses would need to file CTRs on the receipt or withdrawal by any person of more than $10,000 in cash per day. Similarly, any person or entity engaged in a non-financial trade or business would need to report transactions in which they receive more than $10,000 in cash and other monetary instruments for the purchase of goods or services on FinCEN Form 8300 (Report of Cash Payments Over $10,000 Received in a Trade or Business). A business engaged in marijuana-related activity may not be treated as a non-listed business under 31 C.F.R. § 1020.315(e)(8), and therefore, is not eligible for consideration for an exemption with respect to a bank's CTR obligations under 31 C.F.R. § 1020.315(b)(6).

* * * * *

FinCEN's enforcement priorities in connection with this guidance will focus on matters of systemic or significant failures, and not isolated lapses in technical compliance. Financial institutions with questions about this guidance are encouraged to contact FinCEN's Resource Center at (800) 767-2825, where industry questions can be addressed and monitored for the purpose of providing any necessary additional guidance.

Questions for the Record for FinCEN Acting Director Jamal El-Hindi
House Committee on Financial Services
Hearing before the Subcommittee on Terrorism and Illicit Finance entitled
"Safeguarding the Financial System from Terrorist Financing"
Thursday, April 27, 2017

Questions for the Record Submission from Representative Steve Pearce (NM-2)

Analysis and Analytics

Question 1: Can you describe FinCEN's analytic process for financial intelligence?

Response: FinCEN analyzes the reporting it receives and produces strategic and tactical financial intelligence for stakeholders, including Treasury policymakers, law enforcement, regulators, FinCEN's counterpart foreign financial intelligence units (FIUs), other U.S. agency partners, and the regulated industry. Most of FinCEN's analytic work is collaborative and combines reporting to FinCEN with open source information, data, and reporting from law enforcement, other U.S. government agencies, and foreign partners to identify vulnerabilities and risks to the U.S. financial system. Further, FinCEN analyzes emerging financial crime trends, cybercrime, terrorist financing and money laundering networks, regulatory violations, and other illicit finance methodologies.

Question 2: Is the Intelligence Division the only part of FinCEN that conducts analysis, or are there other parts of FinCEN that conduct analysis?

Response: FinCEN's Intelligence Division focuses primarily on analysis, with other divisions also performing analysis to inform specific actions. For example, FinCEN's Enforcement Division undertakes various forms of analysis in the development of specific enforcement matters and investigations, including actions under Section 311 of the USA PATRIOT Act. Analysis is coordinated across FinCEN.

Question 3: Can you explain your work with DARPA, or the Defense Advanced Research Projects Agency, to develop large scale data analysis or open source tools to utilize your BSA data?

Response: FinCEN has partnered with Defense Advanced Research Projects Agency (DARPA) to develop specific data analytic tools and techniques to enhance our organization's advanced analytic capabilities. Over the past two years, FinCEN has worked with DARPA to develop and transition three cutting edge, open-source analytic tools into the FinCEN environment. The tools have provided FinCEN with the capability to conduct geospatial analysis of Bank Secrecy Act

(BSA) filing patterns by countries and regions, explore and analyze illicit finance networks, and visualize transactional flow data to trace money movements by illicit actors.

A. How often are these tools used?

Response: The DARPA tools are available to all FinCEN users (with appropriate mission need) and are used on a varying basis to support projects which benefit from the specific analytic technique the tool(s) provide. DARPA tools have enabled useful analytic products, such as a broad geographic trends and geospatial analysis to benchmark financial activity

Question 4: What types of advanced data analytics programs does FinCEN utilize currently? What is planned in the immediate future?

Response: FinCEN's analytical program has a "toolkit" of tools and capabilities to span the multiple types of analysis required to perform FinCEN's mission. Tools and capabilities include: fast response tactical queries with ambiguous searching, multi-step data manipulation and analysis methods, forecasting and prediction, anomaly detection, network visualization, and automated rules engines. Near-term future efforts include expanding the types and complexity of the models to detect illicit activity, emerging trends, and anomalies; expansion of unstructured data capabilities; and, expanding processing technology and capacity for "Big Data" and machine analysis.

Question 5: Does FinCEN report on the commonalities found between SARs, namely these common items?

- **Addresses**
- **ID numbers**
- **Phone numbers**
- **E-mail addresses**
- **IP addresses**

Response: Yes, FinCEN identifies common indicators, such as those identified above, in its analysis of financial crimes.

A. Does FinCEN proactively analyze or cross-reference SARs for the above common attributes and share with law enforcement for further investigations?

Response: Yes, FinCEN proactively analyzes and cross-references indicators reported in suspicious activity reports (SAR) for their commonalities, producing network analyses in collaboration with law enforcement partners.

Question 6: You mentioned in your written testimony that FinCEN receives 55,000 new filings each day, and that FinCEN collects more than just routinely filed BSA data, like Geographic Targeting Orders, 314(a) requests, and Foreign Financial Agency data. Does all of that non-routine data also get incorporated into the same database as the BSA data so that law enforcement and others with FinCEN access can search all of that data?

Response: The "routine" BSA data is available to law enforcement and regulators generally within one business day of receipt. The "non-routine" data is made available to law enforcement based on the reason and type of request. For example, Geographic Targeting Orders (GTO) usually require filing on current BSA forms which are made available to law enforcement the same as "routine" BSA data. 314(a) requests are initiated and justified for a particular law enforcement case. When data is received from the financial institution(s), the law enforcement requestor is informed new information is available and the information is provided. Foreign Financial Agency (FFA) data is shared with the partner stakeholders associated with the effort, but not to all state, local, and federal law enforcement.

Question 7: What software tools does FinCEN use to conduct its analysis?

Response: FinCEN uses a variety of software tools. Due to sensitivities with sources and methods, we would be happy to discuss the portfolio of tools and capabilities in a non-public venue.

A. Please describe the amounts of money spent for each of the past five fiscal years, including FY 2017, which FinCEN spends on analytic tool development, support, and upkeep, including money spent for contractors.

Response: FinCEN's Information Technology (IT) Modernization program was established to securely collect, store, and disseminate BSA data and is the foundation for FinCEN's analytics. Annually, FinCEN allocates approximately $1 million in development dollars to invest in new analytic and/or data sharing capabilities, and spends around $300,000 in maintenance costs for software and tools. In addition, FinCEN spends approximately $7 million in contractor support costs ($3.6 million for technical support, security integration, and operations; $4.2 million for direct analytic project support).

B. Does FinCEN's technology posture allow for the use of new analytic tools or incorporation of new data sources?

Response: Yes, FinCEN's architecture was designed to be flexible to accommodate our constantly changing threat environment and incorporate new tools or data sources as the need for new business capabilities are identified.

C. Does FinCEN identify, test, evaluate, deploy, and utilize new data analysis tools, techniques, and best practices from commercial or other sources? If so, how?

Response: FinCEN uses a combination of commercially available and custom developed analytic tools and capabilities to support the analysis of BSA data. FinCEN continuously evaluates emerging data analytics technologies to determine if there are new capabilities that would assist the organization in exploiting the information reported in BSA filings. FinCEN conducts market research and assessment of peer agencies and industry to identify tools, techniques, and best practices.

D. Which division is responsible for the identification, testing, evaluation, deployment, and utilization of new analytic tools, techniques, and best practices?

Response: FinCEN's Intelligence, Enforcement, and Technology Divisions are responsible for working together to identify, test, evaluate, and deploy new analytic technologies. Other divisions are incorporated into this process on an as-needed basis.

E. Describe the process and time required to deploy and use an analytic tool, technique, or best practice from the initial identification to its widespread use.

Response: New analytical techniques and best practices can be deployed very quickly, in some cases on the order of days, after the techniques/practices are approved. All such tools go through a system development lifecycle. Depending on the technology and the impact to other systems, potential security risks, and infrastructure changes, new capabilities can be deployed very rapidly or may take several months to fully deploy.

F. Does FinCEN collaborate on analysis and the acquisition of technologies and analytic tools with other parts of the Treasury Department that engage in similar analysis of the BSA, such as the Internal Revenue Service?

Response: FinCEN is in collaboration with other parts of the Treasury Department through FinCEN's Data Management Council, Treasury's Chief Information Officer, and the Office of Terrorism and Financial Intelligence (TFI). The Data Management Council includes FinCEN's regulator and law enforcement stakeholders (including the Office of the Comptroller of the Currency and the Internal Revenue Service) and provides input on BSA data and system features. The Treasury interaction includes direction, oversight, and enterprise architecture initiatives across the Bureaus.

Question 8: What training or assistance currently is provided to analysts regarding FinCEN's analytic tools?

Response: Training is provided through on-line training, job aids, "brown-bag" sessions, and formal classes and seminars. In addition, contractor support is provided for both functional support questions such as "How do I?" as well as data science modeling.

FinCEN has an extensive Analyst career-path training in addition to the training and assistance for the tools.

Question 9: Do the analytic tools currently used at FinCEN provide any of the following capabilities?

- **Trend analysis and discovery**
- **Real-time monitoring and alerts**
- **Machine learning**
- **Entity resolution and data matching**
- **Searches of all FinCEN data**
- **Searches of non-FinCEN data, such as media reporting, commercial databases, and open source data**
- **Ability to add/upload data**
- **Ability to share data and analyses between analysts**

Response: Yes, FinCEN's analytical tools provide trend analysis and discovery; real-time monitoring and alerts; machine learning; entity resolution and data matching; search capability for FinCEN data and non-FinCEN data sources; and the ability to upload and share data. The level of capacity varies. Due to sensitive sources and methods issues, we would be happy to discuss our specific analytical tools and capabilities with you in a non-public venue.

Question 10: Please describe the analytic production cycle, particularly the amount of time required to conduct adequate research using FinCEN's current suite of analytic tools.

Response: FinCEN's analytic production cycle relies on financial intelligence requirements generated by FinCEN priority issues and the needs of our various stakeholders in the law enforcement, intelligence, policy, and industry communities. FinCEN's analyst teams use these requirements to collect information from the BSA databases and conduct additional research using all of the information sources available to the bureau, including law enforcement databases, commercial data, and other government information.

Depending on the specific topic, FinCEN analysts author analytic products ranging from tactical case support to strategic assessments of an illicit finance threat or vulnerability. Some products may move through this analytic cycle in a matter of a few days or weeks, while more complex assessments involving large volumes of data may require additional time to complete.

Question 11: Does FinCEN currently have access to all the tools, data sources, information systems, and facilities that it needs to conduct its analytic mission effectively?

- **If not, what else does FinCEN need?**
  - **Tools?**
  - **Data sources?**
  - **Information systems?**
  - **Facilities?**
- **What steps is FinCEN taking to address these gaps?**

Response: FinCEN has broad access to tools, data sources, information systems and facilities to conduct its analytic mission. In addition, FinCEN works to continually adapt to emerging threats and requirements as they evolve. This continual process facilitates the ability to adjust resources, introduce new techniques, tools, data sources, and support mechanisms. One of FinCEN's strengths is being agile with the ability to prioritize and execute initiatives.

Question 12: Does FinCEN incorporate other data sources into its analysis, such as open source data, commercial databases, and classified information?

Response: Yes, FinCEN incorporates various data sources into its analysis, including open source data, commercial databases and classified information.

A. How does FinCEN access classified information?

Response: FinCEN has access to classified systems, and we would be happy to provide additional detail with regard to how we access such systems in a non-public setting.

B. Does FinCEN rely on the Office of Intelligence and Analysis for classified research, or is FinCEN able to conduct its own classified research?

Response: Both. FinCEN staff with access to classified systems conduct their own research. FinCEN also works with the Office of Intelligence and Analysis (OIA) on classified research.

Question 13: How does FinCEN choose its business rules?

Response: FinCEN employs automated business rules to combat our most significant money laundering and terrorist financing threats. The rules are developed using subject matter expertise and information collected from FinCEN analysts, law enforcement partners, and external stakeholders. The rules align with FinCEN's six priority areas including transnational security threats, cybercrime, transnational organized crime, significant fraud, compromised financial institutions, and third party money launderers.

A. How many rules are currently run? What are the search terms for these particular rules?

Response: Since 2014, FinCEN has deployed more than 95 business rules, of which 62 are currently active. The rules range in complexity from traditional "watch list" rules designed to identify known illicit actors to complex, multi-variable, weighted rule sets capable of identifying emerging illicit activity. The rules search the BSA reporting for key terms, entities, and typologies.

B. Do these rules inform Flash Reports?

Response: FinCEN has a number of business rules designed to identify illicit financial activity associated with both domestic and international terrorism. These rules form the basis for FinCEN's Intelligence Flash Reports. Output from the rules is screened on a daily basis and the most valuable intelligence is selected for inclusion in FinCEN's Flash Reports.

C. How are these reports utilized? Who utilizes them?

Response: Flash Reports provide critical financial intelligence to FinCEN's domestic law enforcement stakeholders, the intelligence community, and FIU partners around the world. Terrorist financing-related Flash Reports assist law enforcement efforts aimed at cutting off terrorist groups' sources of revenue, preventing terrorist groups' access to the international financial system, identifying unknown foreign terrorist fighters, and identifying information related to known actors. The Flash Reports direct law enforcement's attention to particular reporting in the database. The reports are provided for financial intelligence purposes to alert about possible threats and to assist in ongoing investigations.

D. How is all of this information processed and communicated to law enforcement authorities?

Response: FinCEN communicates the financial intelligence it receives (1) by providing both direct access to the BSA filings it receives and (2) by creating a variety of finished products for our federal, state, local, tribal, and foreign law enforcement partners. These law enforcement partners receive products ranging from brief reports on filings of note to strategic analyses of illicit financing methodologies through various mechanisms: encrypted email; through a searchable repository on the FinCEN portal; and a FinCEN special interest group on the Federal Bureau of Investigation's (FBI) Law Enforcement Enterprise Portal (LEEP). FinCEN also works closely with Treasury Department's intelligence community component, OIA, to disseminate information from select BSA reports to national security partners via classified networks. Finally,

FinCEN oversees the receipt and processing of several thousands of requests for information and information exchanges in support of our law enforcement, regulatory, national security, and international partners (i.e., foreign FIUs) via the Egmont Secure Web (ESW) annually.

E. How many "queries" or requests for information does FinCEN staff handle each day?

Response: In FY 2017, FinCEN received:

- 1,017 (3.9 per day) Requests for Information from Egmont FIU partners
- 1,142 (4.4 per day) Spontaneous Disclosures of Information from Egmont FIU partners
- 1,882 (7.2 per day) Requests for Suspicious Transaction Report Supporting Documents from U.S. Requesters (e.g., law enforcement, regulators, FinCEN) and Egmont FIU Partners
- 413 (1.6 per day) Requests from U.S. Requesters to Egmont FIU partners
- 396 (1.5 per day) 314(a) requests
- 38 (.2 per day) Requests for BSA Certified Records
- 18,130 (69 per day) Regulatory Guidance Inquiries

F. How do outside agencies, like the U.S. Customs and Border Patrol (CBP) or the Federal Bureau of Investigation (FBI), utilize Flash Reports?

Response: Flash Reports are one method by which FinCEN proactively disseminates BSA analysis to our partners. These reports are intended to serve as lead information for our partners, including CBP and FBI.

Question 14: How many finished intelligence products does FinCEN produce? How are those disseminated to other agencies? Which agencies does FinCEN share its finished products with?

Response: In FY 2017, FinCEN's Intelligence Division produced 2,950 products of all types, including, but not limited to, Intelligence Flashes, Egmont (foreign FIU) responses, 238 The Committee on Foreign Investment in the United States (CFIUS) responses, Investigative Memos, Intelligence Assessments, and Executive Alerts. The total number of Intelligence Division products produced in FY 2016 was 2,931. FinCEN disseminates these products to a broad list of customers through various mechanisms: (1) encrypted email; (2) through a searchable repository available to all 11,000 users of the FinCEN portal; (3) via the ESW to our 156 international partner FIUs; and (4) via a FinCEN special interest group on the FBI's LEEP. FinCEN also works closely with OIA, Treasury Department's intelligence community component, to

disseminate information from select BSA reports to our national security partners via classified networks. We currently share our products with federal law enforcement agencies and inspectors general; regulatory agencies; state, local, and tribal law enforcement organizations; the U.S. intelligence community; and international partners.

Question 15: Please provide the Subcommittee with examples of FinCEN's analytic product line, including Flash Reports. The Subcommittee would be interested in reports examining terrorist financing, cyber-crime, virtual currencies, drug trafficking, human trafficking, transnational organized crime, and other illicit finance methodologies.

Response: Due to the sensitive nature of BSA information, we would be happy to discuss these products in a non-public venue.

Question 16: We hear a lot about data analytics. How does FinCEN plan to incorporate some of today's modern technologies?

Response: As part of the technology roadmap and review process, FinCEN identifies, evaluates, pilots, and implements new technologies. Some of those technologies are adapted from external agencies such as DARPA (please see response to Question 3). FinCEN is on-track to be the first Treasury Department Bureau using big data technologies in a production system in the classified cloud environment.

Question 17: Has FinCEN met with any outside organizations that use artificial intelligence instead of rules based software to identify anomalous behavior?

Response: Yes, FinCEN has met with external organizations and attended industry meetings regarding the application of artificial intelligence (AI). The evolution of rules based, to machine learning, to potential AI is part of the technology roadmap for analytical capabilities.

Question 18: What work - analytic, regulatory, and otherwise - is FinCEN doing, or does it anticipate doing, on emerging payment systems and virtual currencies?

Response: FinCEN actively studies emerging payment systems and virtual currencies to identify how they may be exploited for financial crime, terrorist financing, and money laundering. FinCEN analysts are recognized as thought leaders on the potential illicit uses of new financial technologies, and are frequently called upon to provide training on emerging payment and virtual currency issues to federal law enforcement agencies, other U.S. government agencies, and international partners. FinCEN has supported several dozen law enforcement cases involving the exploitation of virtual currency systems, and publishes periodic analytic reports assessing criminal methods and vulnerabilities in emerging payment systems.

Emerging payment systems and convertible virtual currencies are covered by the general recordkeeping, reporting, and transaction monitoring requirements applicable to money services businesses (MSBs). In 2013, FinCEN provided guidance on how virtual currency administrators, exchangers, and users would be treated under the BSA. Since that time, FinCEN has continued to conduct outreach, provide guidance, and issue administrative rulings as this sector evolves. FinCEN continues to supervise virtual currency providers and exchangers.

FinCEN has also aggressively enforced its authorities in the virtual currency space. For example, in coordination with the U.S. Attorney's Office for the Northern District of California, FinCEN assessed a $110,003,314 civil money penalty on July 27, 2017, against Canton Business Corporation (BTC-e), an internet-based, foreign-located money transmitter that exchanged fiat and convertible virtual currencies for willfully violating U.S. anti-money laundering laws. BTC-e facilitated millions of dollars of transactions involving ransomware, computer hacking, identity theft, tax refund fraud schemes, public corruption, and drug trafficking while collecting little to no information on its customers. BTC-e and one of its operators were also indicted in July 2017 for operating an unlicensed money services business, money laundering, and related crimes.

Office of Intelligence and Analysis

Question 19: Does the Office of Intelligence and Analysis (OIA) provide support to FinCEN? How? Please provide specific examples of the support provided by OIA – analytic and non-analytic – to FinCEN.

Response: FinCEN works closely with OIA, Treasury's intelligence community element, to disseminate information from select BSA reports to our national security partners via classified networks. The Management Division works closely with OIA on security matters, and OIA is consulted on a general basis with respect to all Treasury interactions with the U.S. intelligence community. For example, OIA is responsible for administering access controls that make it possible for other parts of Treasury, including FinCEN, to access various sets of classified information. OIA also provides intelligence support to FinCEN's Enforcement Division in connection with its investigations of foreign money laundering threats. In addition, OIA provides FinCEN senior leadership with daily intelligence readbooks, to include OIA intelligence products of interest.

A. Is the support that OIA currently provides to FinCEN sufficient for FinCEN's needs?

Response: FinCEN and OIA have been working on ensuring sufficient levels of FinCEN access to, and use of, classified information to add context to FinCEN's analysis of BSA information,

while at the same time addressing appropriate safeguards with respect to access to classified information generally.

B. What other support from OIA does FinCEN need, if any?

Response: OIA's analytic products provide FinCEN and others with greater context for pursuing global money launderers and terrorist financiers. OIA also drives IC collection to support Treasury efforts, including those of FinCEN.

Question 20: In a letter to Michael Fitzpatrick, then-Chairman of the and House Financial Services Committee's Task Force to Investigate Terrorism Finance, and Sean Duffy, then-Chairman of the Subcommittee on Oversight and Investigations, the Treasury Department's Office of Legislative Affairs stated that the purpose of the proposed realignment of 15 personnel with BSA analytical experience from FinCEN to OIA was being undertaken for the purpose of providing FinCEN better support from the intelligence community and more sophisticated analysis. What sophisticated analysis and support does OIA provide to FinCEN?

Response: OIA's analytic production is informed by the all-source intelligence analysis it undertakes on a wide range of topics of interest to Treasury senior policymakers, including those at FinCEN. FinCEN personnel with appropriate clearances have access to OIA products on Treasury's classified portal. OIA is also postured to provide tailored support to FinCEN to address key intelligence questions that pertain to FinCEN's mission.

A. What is the current status of this realignment?

Response: No FinCEN personnel were ultimately detailed to OIA in connection with the realignment.

Question 21: Does FinCEN provide support to OIA? How? Please provide specific examples of support provided to OIA – analytic and non-analytic – from FinCEN.

Response: FinCEN provides large BSA dataset information to OIA, and OIA has access to FinCEN Query to do research on most issues. Under certain circumstances, and in accordance with 31 U.S.C. 5319 and 31 U.S.C. 310, FinCEN provides to OIA information obtained pursuant to FinCEN's authorities. Moreover, FinCEN in collaboration with TFI created a training series on illicit finance methodologies and emerging payment systems designed for OIA and TFI officers. This effort benefits from FinCEN's continued research on both legacy and emerging payment systems, resulting in written products and complimentary training modules. The TFI-targeted series offers on-site presentations geared to threat finance issues and problem sets of

interest to TFI analysts, policy makers, and other full-time employees. FinCEN continues to work with TFI and OIA to solicit ideas for future research and products, and to support expertise building within and beyond TFI.

Question 22: Does FinCEN still intend to pursue this realignment of intelligence analysts to OIA? If so, why has FinCEN asked for $1.5 million for contractor support, when it can afford to lose 15 FTE analysts?

Response: As noted above, no FinCEN personnel were ultimately detailed to OIA in connection with the proposed realignment. FinCEN does not intend to pursue the proposed realignment.

Question 23: Has FinCEN notified Secretary Mnuchin and other officials of the new administration about the proposed realignment? Does FinCEN intend to do this?

Response: Treasury Department's current leadership, including the Secretary, are generally aware of the proposals regarding last year's proposed realignment.

Question 24: You mentioned in your oral testimony that the goal of the realignment was for TFI to work better together. Please describe how FinCEN currently collaborates with OIA, OFAC, TFFC, and the TFI Front Office, including details about its participation in Integrated Mission Teams.

Response: FinCEN works with its sister components reporting to the Under Secretary for Terrorism and Financial Intelligence in a number of ways. FinCEN's data and analysis and FinCEN's tools are used together with the tools and efforts of the other components on high-profile priority issues such as those pertaining to Iran, North Korea, other countries or regimes of concern, and terrorism. Integrated teams involving personnel from multiple TFI components work to ensure greater coordination and collaboration of efforts on such topics. FinCEN also works with the Office of Terrorist Financing and Financial Crimes (TFFC) on broader regulatory and policy issues. The TFI Front Office works to ensure that all component parts are provided with strategic direction on matters of greatest concern. A key element of TFI's continued success in addressing national security challenges is ensuring that the various components are properly integrated, working closely together, and deploying the tools and authorities best suited to each challenge.

A. **How would sending 15 intelligence analysts impact the ability of FinCEN's Intelligence Division to conduct its mission? Would FinCEN need to reduce its analytic production?**

Response: As noted above, no FinCEN personnel were ultimately detailed to OIA in connection with the proposed realignment.

Question 25: The Subcommittee understands that since at least September 2016 there has been a significant decline in the numbers of security clearances, classified network accounts, and access to classified research, analysis, and collaboration tools granted by OIA to FinCEN. Is this still the case?

Response: Since September 2016, the total number of FinCEN personnel that OIA has indoctrinated into SCI has increased by approximately 16% (from 153 to 178 personnel), and the total number of accounts for Treasury's Foreign Intelligence Network (TS/SCI computer network) that OIA has granted to FinCEN personnel has grown by 32% (from 75 to 99 accounts).

A. You just testified that roughly half of the 70 vacancies at FinCEN are in the "active recruitment process" but awaiting security clearance processing. What is the reason for this slowdown?

Response: We understand that the National Background Investigation Bureau (NBIB) at the Office of Personnel Management is working through a backlog of background investigations. The Treasury Department, including FinCEN, is dependent upon NBIB's background investigation completions prior to being able to make adjudicative decisions. Once the investigations are received from OPM, the median average time FinCEN took to adjudicate its collateral clearances in 2016, was 26 days, according to OPM records.

B. Who made the decision to halt the issuance of new clearances, accounts, and accesses?

Response: Neither OIA nor FinCEN is aware of a decision to halt the issuance of new clearances, accounts, or accesses.

C. How many FinCEN employees have been affected by this decrease?

Response: As stated earlier, the total number of FinCEN personnel indoctrinated into SCI and with TFIN accounts has increased, not decreased, since September 2016. Nine FinCEN candidates have accepted tentative job offers and are awaiting security clearances/accesses required to onboard. The NBIB security background investigation backlog is impacting FinCEN's ability to onboard.

D. How many employees have requested clearances, accounts, and access since September 2016? How many clearances, classified accounts, and accesses were issued of this total? How many clearances, classified accounts, and accesses were denied of this total? How many clearances, classified accounts, and accesses are still pending of this total?

Response:

(Since Sept 1, 2016)	Clearances[1]	Accounts (TFIN)	Accesses (SCI)
Requested	40	69	94
Issued	21	63	78
Pending	18*	6	16
Denied	1	0	0

As of May 7, 2018

*Of the 18 pending: 13 are pending the completion of Office of Personnel Management/National Background Investigations Bureau investigative activities; three are pending Office of Security Programs; two are cleared but pending Entry on Duty and the issuance of clearance

E. How has the slowdown in these approvals affected FinCEN's analytic and enforcement missions?

Response: All of FinCEN's divisions and organizations are affected by lengthy background investigations necessitated by FinCEN's security clearance requirements. Although FinCEN is not at full strength, we utilize appropriated funds for a variety of support contracts that allow us to leverage our Federal work force to meet the growing demand for FinCEN data and emerging threats to the financial system. These contracts provide case support and functional specialists to support a number of Divisions, cyber security experts to respond to the expanding cyber threat, human resource expertise to support the hiring surge, and data analysis and expertise support to intelligence analysts

F. What number of staff clearances, accounts, and accesses does FinCEN believe is necessary to fulfill its analytic and enforcement missions?

[1] NOTE: FinCEN has historically conducted its own collateral security clearance adjudications with OIA adjudicating its SCI access.

Response: FinCEN recently conducted a position designation exercise as mandated by the Office of the Director of National Intelligence to determine the proper position designations for each position required to accomplish FinCEN's mission. 19 positions were downgraded as a result of this exercise (e.g. from Top Secret to Secret or Public Trust, or from Secret to Public Trust). FinCEN's national security and law enforcement roles necessitate 329 of 339 positions to be sensitive, national security positions.

Question 26: Does FinCEN produce any products or analysis jointly with OIA?

Response: Although FinCEN and OIA have different primary customers, there are opportunities for collaboration in the development of certain products and some overlaps in the customer base. For example, both components serve TFI seniors and products may be read externally by similar customers.

Question 27: Has FinCEN delineated and differentiated its analytic responsibilities with those of OIA in a document called Treasury Intelligence Enterprise Management Guidelines?

Response: Former Acting Under Secretary Adam Szubin disseminated guidance across TFI regarding Treasury's intelligence activities. The guidance was coordinated with all TFI components. The guidance codifies OIA's role and delineates two categories of Treasury intelligence activities: those that must be coordinated with OIA and those that are to be conducted solely by OIA.

A. Who initiated this document?

Response: The guidance was drafted by OIA and subject to multiple rounds of coordination with all TFI components.

B. Who approved this document?

Response: The heads of all TFI components signed off on the document, which was ultimately approved by Acting U/S Szubin.

C. Has this document been shared with and approved by Secretary Mnuchin and others at Treasury?

Response: Treasury's senior leadership is aware of this guidance.

D. What restrictions were placed on FinCEN by this document?

Response: The guidelines help to coordinate and deconflict the activities of TFI components. For example, FinCEN is able to ask clarifying questions to the Intelligence Community (IC) about existing IC reporting, but requests for IC collection, analysis, and intelligence and counterintelligence needs are routed through OIA to ensure that FinCEN's requests of the IC are tracked and deconflicted with other Treasury intelligence needs.

E. Does this document prevent FinCEN from interacting directly with its customers and partners in the Intelligence Community?

Response: FinCEN's relationships with intelligence community agencies are outlined in signed Memorandum of Understanding documents with those agencies.

F. Does this document hinder FinCEN from fulfilling its statutory mission?

Response: No.

Question 28: What access does OIA have to access BSA data, including standard filings as well as data collected under FinCEN's special measures authority?

Response: OIA has access to perform specific searches of BSA data using FinCEN Query.

A. How many user accounts are allocated to OIA?

Response: Currently, 31 OIA employees have BSA access accounts.

Question 29: Has FinCEN verified that OIA, as a member of the Intelligence Community, has the authority to receive, process, store, analyze, and disseminate the information on U.S. Persons contained in the BSA data to which FinCEN has given OIA access?

Response: By statute FinCEN is directed to share information with the intelligence community. The intelligence community is responsible for ensuring that it appropriately uses the information in accordance with applicable requirements.

A. Has FinCEN received or seen a copy of OIA's guidelines for handling U.S. Persons information as required by Executive Order 12333? If so, when? Please provide a copy to the Subcommittee.

Response: Your request for a copy of OIA's guidelines for handling U.S. Persons information has been submitted to OIA for direct response.

B. What safeguards does FinCEN have to protect that personally identifiable information from misuse?

Response: FinCEN has a Privacy Administrator (PA) responsible for implementing the recommendations of the 911 Commission to ensure that the bureau appropriately considers privacy and civil liberties concerns in executing its mission. The FinCEN ensures that appropriate safeguards are integrated into the policies, systems, and processes whereby FinCEN collects, analyzes, and disseminates personally identifiable information (PII). Additionally, the integrity and confidentiality of the PII that FinCEN collects, transmits, maintains, and utilizes is controlled through mechanisms that identify and regulate the appropriate purposes and uses of the data and maintain the individuals' privacy.

The privacy and civil liberty impacts of business and analytical processes and technology usages are documented in internal Privacy Threshold Analyses (PTA) and internet-accessible Privacy Impact Analyses (PIAs). FinCEN's quarterly and annual Federal Information Security Management Act (FISMA) reports for Privacy and the annual Data Mining Report detailing FinCEN privacy practices are sent on a regular basis to Treasury Department's Director of Privacy. These documents and reports also describe the secure architecture and data security tools used in managing FinCEN's technology systems. Additionally, System of Record Notices are reviewed, minimally, every three years and re-published on the internet.

FinCEN has published a directive that mandates policy and procedures for reporting privacy incidents and for breach response. FinCEN's Breach Review Group (BRG) maintains a plan which is used to promptly and efficiently assess the risk created by an incident and to determine its impact to individual privacy rights. The BRG then recommends an appropriate response, appropriate notifications and remediating actions, and uses "lessons learned" to mitigate future threats.

Privacy training and awareness at FinCEN include both formal course materials and promotional awareness of PII safeguarding practices. All staff must complete mandatory, annual privacy training. Situational awareness activities in a variety of delivery formats occur throughout the year along with role-based privacy training as needed.

Facilities and Resources

Question 30: Does FinCEN currently have adequate SCIF space, to include classified computers, classified phones, classified video conference capability, and other such equipment and facilities necessary to conduct its counter terrorist financing mission?

Response: Yes, FinCEN has adequate SCIF facilities.

Question 31: The FY17 Budget Request mentions an efficiency savings of $1.3 million, including reductions in travel. Please provide information adequate to support how FinCEN arrived at this figure. Given FinCEN's close cooperation with international partners, why is FinCEN reducing travel?

Response: The FY 2017 Budget Request proposed $1.3 million in efficiency savings. Of the $1.3 efficiency savings, $550,000 is from commercial database contracts and $750,000 is from re-evaluation or negotiation of other contractual efforts. FinCEN did not reduce travel funding, but has made plans to use travel funds more efficiently.

Data and Data Security

Question 32: What kind of Bank Secrecy Act data does FinCEN compile?

Response: FinCEN compiles data as obtained from the different reports required to be filed under the Bank Secrecy Act:

- FinCEN Suspicious Activity Report (Form 111): Reports made by a financial institution about suspicious or potentially suspicious activity.
- FinCEN Currency Transaction Report (Form 112): Reports for each deposit, withdrawal, exchange of currency, or other payment or transfer, by, through, or to the financial institution which involves a transaction in currency of more than $10,000.
- Form 8300: Reports of cash payments over $10,000 received in a Trade or Business over a twenty-four-hour period. Each person engaged in a trade or business who, in the course of the trade or business, receives more than $10,000 in cash in one transaction or in two or more related transactions, must file Form 8300.
- Currency and other Monetary Instruments Report (CMIR) (Form 105): Reports international transportation or currency and/or other monetary instruments exceeding $10,000.
- Foreign Bank and Financial Accounts (FBAR) (Form 114): Reports financial interest in or signature authority over a foreign financial account. A United States person that has a financial interest in or signature authority over foreign financial accounts must file an FBAR if the aggregate value of the foreign financial accounts exceeds $10,000 at any time during the calendar year.
- Designation of Exempt Persons Report (DoEP) (Form 110): Report to provide an effective means for a bank to exempt eligible customers from currency transaction reporting and to reduce the bank's burden of filing Currency Transaction Reports (CTR). Banks are the only type of financial institutions that may exempt customers from CTR filing requirements.

- Registration of Money Services Business (RMSB) (Form 107): This form provides FinCEN with information that registrants are required to provide in order to be registered and allows MSBs that are required to be registered to provide data that allows their registration to be accepted. Generally, MSBs must register with the Department of the Treasury. However, not all MSBs are required to register. For example, if you are an MSB solely because you are an agent of another MSB, you are not required to register.

Question 33: There is a viewpoint that FinCEN gets "too much" information and thus is unable to sort through it for important indicators of crimes. Could you please address that?

Response: While the volume of BSA reporting has increased, so has FinCEN's capacity to extract valuable information from these reports. For instance, through the use of algorithms, and the alertness of financial institutions, we are now able to identify funds and persons related to potential foreign terrorist fighters that otherwise could have gone unnoticed a decade ago. We constantly seek ways to improve the BSA system's effectiveness and utility.

Question 34: Who at FinCEN looks at the 55,000 reports that come in every day?

Response: FinCEN leverages several different strategies to review the 55,000 BSA filings financial institutions submit on a daily basis. FinCEN employs automated business rules to screen all filings for information associated with our most significant money laundering and terrorist financing threats. Findings from the rules point FinCEN analysts to specific filings for hands-on review and focus efforts on the filings most likely to be related to priority threats. In addition, FinCEN analysts independently execute queries to screen for information associated with their areas of responsibility. Finally, FinCEN has a group of data scientists that conduct analysis using advanced algorithms to surface information associated with entities that are most prevalent in the data or whom may be engaging in sophisticated money laundering, significant fraud, or terrorist financing schemes.

Question 35: Is FinCEN concerned with the number of SARs filed or the quality of SARs filed?

Response: We expect financial institutions to fulfill their regulatory requirements and file the appropriate BSA forms accurately and completely as part of meeting their overall BSA obligations. When systemic errors in a financial institution's CTRs or SARs are identified, FinCEN contacts the financial institution and works with them to develop a program and timeline for correcting the errors.

Question 36: What can be done to address so-called "defensive SAR filing?"

Response: FinCEN has studied the issue of "defensive filing" by reviewing samples of SAR filings and has found little evidence of unnecessary SAR filings. To the contrary, FinCEN believes financial institutions are doing a good job of spotting and reporting suspicious activity that is of high-value to law enforcement. It is worth noting that the value of reporting suspicious activity is multiplied when many financial institutions are watching for, and sharing information on, similar activity. What, in isolation, seems to be a minor report from one institution may, in fact, be illustrative of a broad and dangerous trend when viewed in context of other filings.

Question 37: Can you discuss the various kinds of information collected through FinCEN's special measures authorities, such as Geographic Targeting Orders (GTOs), demand letters, Foreign Financial Agency data, and the like?

Response: A GTO is an order issued by FinCEN under the BSA that imposes additional recordkeeping or reporting requirements on domestic financial institutions or other businesses in a specific geographic area.

A Demand Letter is a request by FinCEN, under 12 U.S.C. § 1829b(b)(3)(C) for records relating to international funds transfers of $3,000 or more. The scope of the requested information can vary depending on the specific circumstances of the request.

A Foreign Financial Agency rule (FFA Rule) is a rulemaking issued by FinCEN under the BSA that imposes additional reporting requirements on domestic financial institutions. The regulation requires identified domestic financial institutions to report transactional information involving identified Foreign Financial Agencies.

A. Does FinCEN have any data to show the effectiveness of the 314(b) program?

Response: Section 314(b) of the USA PATRIOT Act is a voluntary information sharing program. 314(b) provides financial institutions with the ability to share information with one another, under a safe harbor that offers protections from liability, in order to better identify and report potential money laundering or terrorist activities. Since 2012, more than 46,000 BSA filings have been submitted that reference 314(b) information sharing within the narrative of the BSA report. From 2012-2016, the prevalence of terrorist financing SARs referencing 314(b) has increased significantly, from 25 SARs in 2012, to 96 in 2016. This indicates financial institutions are using 314(b) more frequently in their efforts to detect and report suspected terrorist financing.

B. Does FinCEN have any data to show if financial institutions comply or don't comply with incoming 314(b) requests?

Response: No, section 314(b) of the USA PATRIOT Act is a voluntary information sharing program. 314(b) provides financial institutions with the ability to share information with one another, under a safe harbor that offers protections from liability, in order to better identify and report potential money laundering or terrorist activities. FinCEN regulations (31 CFR 1010.540) set forth the requirements that must be satisfied in order to benefit from 314(b) safe harbor protection.

C. Does FinCEN have any plans to make financial institutions accountable if they don't respond to 314(b) requests?

Response: No, 314(b) is a voluntary program that provides financial institutions with the ability to share information with one another, under a safe harbor that offers protections from liability, in order to better identify and report potential money laundering or terrorist activities.

However, FinCEN does monitor for compliance with 314(a) requests. If a determination is made that a financial institution is not in compliance with 314(a), the matter generally would be referred to their federal regulator for action. FinCEN also considers 314(a) compliance as part of its own BSA investigations into financial institutions.

Question 38: Does FinCEN's BSA database include all BSA data, including that information collected under FinCEN's special measures authority?

Response: Currently, FinCEN's System of Record (SOR) only stores the structured data collected via the FinCEN forms noted in the response to Question 32. In some cases, special collections require submitting forms, so in those instances, special collections data is also stored in the SOR. We are in the process of developing the capability and tools to also store the more unstructured special measures data in the SOR. Currently, the more unstructured special measures data is stored on protected share drives.

A. Do law enforcement and others have access to that special measures data?

Response: Where the information collected through a special measure comes to FinCEN via the use of one of FinCEN's standardized formats, special measures data is available to law enforcement and others through FinCEN Query. Unstructured special measures data may be disseminated to law enforcement, if appropriate, on a case-by-case basis.

B. Where is special measures data stored?

Response: Unstructured special measures data is stored on protected share drives within FinCEN.

C. Who controls the storage of special measures data?

Response: FinCEN's Enforcement Division controls the storage of the unstructured special measures data on protected share drives, which are managed by the Technology Division.

D. How is special measures data disseminated?

Response: Unstructured special measures data may be disseminated to law enforcement and other governmental entities, if appropriate, on a case-by-case basis.

E. To whom is special measures data disseminated?

Response: Unstructured special measures data may be disseminated electronically to law enforcement and other governmental entities, if appropriate, on a case-by-case basis.

F. What access controls and data security measures are currently in place protecting special measures data?

Response: In some cases, special collections require submitting forms, so in those instances, special collections data is stored in the SOR and subject to the same controls and data security measures applicable to other BSA information. For unstructured special collections, FinCEN requests that the information be submitted through the Secure Information Sharing System (SISS) that is managed by FinCEN or via password-encrypted files. SISS uses a direct communications path with a multi-step, authentication process for incoming data and that data is scanned for viruses. If a virus is found, it is rejected. If accepted, files are transferred to internal protected share drives. Access to share drives is limited to data owners by an Administrator with data owners controlling access to the data.

Question 39: In your testimony, you mentioned previously that over 10,000 federal, state, and local users have access to the BSA database. How do you ensure that the data is not being misused or improperly shared?

Response: Users of BSA data, both at an organizational and individual level, agree to terms and conditions under Memorandums of Understanding (MOU) executed with FinCEN. At the outset of establishing an MOU and on a periodic basis thereafter, users are provided with BSA Re-Dissemination Guidelines and guidance for properly safeguarding BSA information. Every year, FinCEN makes contact with the more than 400 agencies with BSA data access MOUs. After an electronic review of the agency's use of the system, FinCEN conducts a telephonic inspection.

The FinCEN Query system has built-in query audit logs which capture each user's activity within the BSA system of record. Monthly reports are run to detect certain anomalies within the query audit logs. Mandatory on-line training must be taken by all users prior to their access of the BSA data, including acceptance of a user acknowledgment. This helps FinCEN to ensure all users are aware of the proper use of the data. FinCEN also investigates suspected unauthorized disclosure of BSA information and audits FinCEN employees' use of the BSA data.

Information Technology

Question 40: Does FinCEN have an IT strategy or risk mitigation plan in place to protect against cyber criminals or other threats like the breach of OPM's systems?

Response: FinCEN systems are accredited at the FISMA High level. FinCEN continuously monitors and adapts to emerging threats using risk management. Specific security related information is considered sensitive for public record. FinCEN is willing to brief security information privately, if requested.

Question 41: Have there been any breaches of the BSA database or the Egmont Secure Web?

Response: Specific security related information is considered sensitive for public record. FinCEN is willing to brief security information privately, if requested.

Question 42: Has there been any misuse of the BSA database or the Egmont Secure Web?

Response: Insuring the responsible and proper use of sensitive BSA data is a priority for FinCEN, and, as noted above FinCEN investigates unauthorized disclosures of BSA information. Specific security related information is considered sensitive for public record. FinCEN is willing to brief security information privately, if requested.

Question 43: Have there been any investigations or audits of the BSA system or Egmont Secure Web to gauge possible misuse? Have there been any incidents of misuse or unauthorized sharing of data?

Response: FinCEN has an inspection program, training outreach, and system monitoring capabilities to gauge possible misuse. Potential incidents are investigated by FinCEN Office of Special Investigations. Specific security related information is considered sensitive for public record. FinCEN is willing to brief security information privately, if requested.

Question 44: How does FinCEN protect against the spillage or misuse of personally identifiable information (PII)?

Response: FinCEN systems are accredited at the FISMA High level. FinCEN continuously monitors and adapts to emerging threats using risk management.

Question 45: You mentioned in your testimony that FinCEN completed its Information Technology modernization program in 2014. What strategy and goals is FinCEN pursuing to further modernize, update, and upgrade its information technology capabilities?

Response: FinCEN Technology Division uses roadmap sessions with other FinCEN divisions, as well as an Investment Review process to continually update and enhance mission capabilities supported by technology. Enhancements have included delivering new tools, pilots in Hadoop and other "Big Data" technologies to scale data analysis and allow for new techniques, pilots in Cloud Computing to increase adaptability and decrease implementation time, and increase automation in collection and dissemination processes to reduce cycle time.

Question 46: Can you describe how FinCEN's recent IT project has helped modernize BSA data management?

Response: The IT Modernization project established BSA data management processes such as the Data Management Council, Integrated Project Teams, and governance processes to provide transparency into data management issues and ensure business requirements and impacts were incorporated into the planning and prioritization process. In addition to process improvements, IT Modernization also improved data collection by standardizing data across forms, shifting to a data-centric design, incorporating additional data validations, and implementing technical data standards to increase data quality and increase analytical capability.

Question 47: How do the technological capabilities of other FIUs, such as Australia's AUSTRAC, Canada's FINTRAC, and the Netherlands' FIU, compare to those of FinCEN?

Response: FinCEN coordinates with other FIUs regarding collection and analytical capabilities. The Australian Transaction Reports and Analysis Centre (AUSTRAC), the Financial Transaction and Reports Analysis Centre of Canada (FINTRAC), and the Netherlands' FIU have slightly different operating models and collection requirements. AUSTRAC, FINTRAC, and others have visited FinCEN during their modernization efforts and as part of the Egmont Group, FinCEN is the Vice Chair of the Information Exchange Working Group to lead and exchange technical capabilities.

Question 48: Does FinCEN utilize, or has FinCEN examined utilizing the cloud computing or "as-a-service" model?

Response: Yes, FinCEN is currently working on developing, implementing and obtaining appropriate security accreditations for initial cloud solutions.

Special Measures

Question 49: How does FinCEN decide which entities and individuals to target with its special measures authorities?

Response: The Office of Special Measures within FinCEN's Enforcement Division executes FinCEN's unique enforcement and information request authorities to detect, disrupt, and deter key illicit finance threats, including money launderers, the financial institutions they exploit, and the methods they employ. For example, under Section 311 of the USA PATRIOT Act, FinCEN can identify a foreign financial institution, jurisdiction, class of transactions, or type of account as being of primary money laundering concern. Upon making such a finding, FinCEN may impose one or more of five special measures on U.S. financial institutions, from enhanced recordkeeping and reporting requirements up to prohibitions on correspondent account access.

In making such a finding and determining which special measure is most appropriate, FinCEN considers the factors outlined in the statute. For example, for a particular jurisdiction, FinCEN may consider jurisdictional factors such as evidence that organized criminal groups, international terrorists, or entities involved in the proliferation of weapons of mass destruction or missiles have transacted business in that jurisdiction. For a foreign financial institution, class of transaction, or type of account, FinCEN may consider factors such as the extent to which the subject of the finding is used to facilitate or promote money laundering or is used for legitimate business purposes. FinCEN is also required to consult with the Attorney General, the Secretary of State, and the heads of the federal functional regulators.

Question 50: What does FinCEN do with the special measures information?

Response: FinCEN collects a variety of information under the BSA outside the standard filings that covered financial institutions make as a matter of course, such as SARs and CTRs. For example, in order to further the purposes of the Bank Secrecy Act and prevent evasions thereof, FinCEN may impose temporary enhanced reporting requirements on financial or nonfinancial businesses under Geographic Targeting Orders pursuant to 31 U.S.C. 5326. FinCEN can also collect certain transactional records under special authorities to request information, such as the Foreign Financial Agency authority under 31 U.S.C. 5314 and the authority to obtain certain international funds transfers under 12 U.S.C. 1829b. The use of these authorities depends on the

specific facts and circumstances of each matter, but in general, FinCEN may exercise these authorities to support its own investigations; to identify money laundering trends and typologies that can be shared with other agencies or the private sector; and to assist law enforcement or other U.S. government entities in furtherance of a criminal, tax, or regulatory investigation or proceeding, or in the conduct of intelligence or counterintelligence activities to protect against international terrorism.

Question 51: How is special measures information actually collected – how do financial institutions and other responsive entities send that information to FinCEN?

Response: FinCEN generally instructs financial institutions and businesses subject to a special information request to submit the information to FinCEN via the standard Bank Secrecy Act database (often using pre-existing forms, such as the FinCEN Form 8300) or through FinCEN's SISS, which is a secure mechanism to communicate with financial institutions.

Question 52: How is the special measures information stored, analyzed, and disseminated?

Response: Reports that are responsive to special information requests that are submitted via the standard Bank Secrecy Act database are stored in the same manner as SARs, CTRS, and other such forms. Such reports are also available for analysis to law enforcement and other users with access to the BSA database. Information sent through FinCEN's SISS is stored on FinCEN's servers.

Question 53: To whom is special measures information disseminated, and in what form?

Response: FinCEN may disseminate reports filed under the Bank Secrecy Act, including information obtained pursuant to its special authorities to request information, to other governmental agencies, including law enforcement and regulators, in accordance with 31 USC 5319 and 31 USC 310. FinCEN may disseminate such information electronically with explicit warnings that the information may not be released, disseminated, disclosed, or transmitted outside the receiving organization without the prior, written approval of FinCEN.

Geographic Targeting Orders (GTOs)

Question 54: Can you speak to the law enforcement concerns regarding the potential misuse of anonymous shell companies for illicit purposes in the real estate sector?
Response: Shell companies generally include non-publicly traded corporations and limited liability companies that typically have no physical presence and generate little to no independent economic value. Many shell companies are formed for legitimate tax and liability purposes, but the anonymity they can provide may also be abused by illicit actors seeking to hide their

involvement in a particular transaction. The misuse of shell companies to launder money is a systemic concern for law enforcement and regulators across the financial system, but it is particularly problematic in the "all-cash" (i.e., purchases of real estate made without external financing or a mortgage) segment of the real estate market, which currently has relatively few anti-money laundering protections.

In January 2016, FinCEN issued GTOs to require U.S. title insurance companies to report beneficial ownership information on legal entities, including shell companies, used to purchase certain luxury residential real estate in Manhattan and Miami—specifically, luxury residential property purchased by a shell company without a bank loan and made at least in part using a cashier's check or similar instrument. In July 2016 and February 2017, FinCEN reissued the original GTOs and extended coverage to all boroughs of New York City, two additional counties in the Miami metropolitan area, five counties in California (including Los Angeles, San Francisco, and San Diego), and the Texas county that includes San Antonio. Following the enactment of Countering America's Adversaries through Sanctions Act in August 2017, FinCEN issued revised GTOs to capture a broader range of transactions and included transactions involving wire transfers. FinCEN also expanded the GTOs to include transactions conducted in the City and County of Honolulu, Hawaii. These expanded GTOs will further help law enforcement and inform FinCEN's future efforts to assess and combat the money laundering risks associated with luxury residential real estate purchases.

In March 2018, FinCEN extended the GTO in response to the useful information that we have been receiving under the new authority to include wire transfers and we continue to define methods to address the vulnerabilities of this sector.

Question 55: President Trump recently extended Geographic Targeting Orders to all title companies in six major metropolitan areas. Can you explain what these GTOs have provided?

Response: At the time of the most recent renewal, approximately 30 percent of the real estate transactions reported under the GTOs involved a beneficial owner or purchaser representative who had previously been the subject of a SAR. In other words, the beneficial owners or purchaser representatives in a significant portion of transactions reported under the GTO had been previously connected to suspicious activity. As a result of the attention generated by the GTOs, we have seen additional SAR filings related to potential money laundering involving real estate. In total, these SARs, along with the information generated by the GTOs, are advancing law enforcement's ability to identify potentially illicit activity and are helping inform FinCEN's broader AML approach towards the real estate sector.

Question 56: When you say that 30 percent of transactions covered by these GTOs "involved a beneficial owner ... that was also the subject of a previous suspicious activity report," does that mean they are all illicit financiers?

Response: No. A financial institution may be required to file a SAR if it knows, suspects, or has reason to suspect a transaction conducted or attempted by, at, or through the financial institution involves funds derived from illegal activity; attempts to disguise funds derived from illegal activity; is designed to evade regulations promulgated under the BSA; lacks a business or apparent lawful purpose; or involves the use of the financial institution to facilitate criminal activity. See, e.g., 31 C.F.R. 1020.320. The filing of a SAR does not necessarily mean that the subject engaged in criminal activity, only that the filing institution identified suspicious activity.

A. How many transactions were covered by the GTO?

Response: As of December 2017, FinCEN has received 764 reports of covered transactions.

B. And 30% of that figure is...?

Response: As of December 2017, FinCEN has received 243 reports of covered transactions that involved a beneficial owner or purchaser representative who had previously been the subject of a SAR.

Question 57: Real estate purchases funded solely through wire transfers are not included in the GTO, is that correct? Couldn't a savvy financier easily navigate around FinCEN's rules?

Response: On August 2, legislation was signed into law that closed the wire transfer loophole in the GTO authority. Purchases funded through wire transfers must be reported pursuant to FinCEN's most recent real estate GTOs issued on August 22, 2017, and the March 19, 2018 GTOs.

Question 58: Are these wire transfers captured in any of the other reporting requirements?

Response: As noted above, purchases funded through wire transfers must be reported pursuant to FinCEN's most recent real estate GTOs issued on August 22, 2017, and the March 19, 2018 GTOs.

Question 59: Has FinCEN conducted any analysis on the possibility of money laundering that employs a transaction involving outside financing?

Response: For the Real Estate GTOs, FinCEN's focus was on all-cash transactions because in situations where bank financing is involved—even a small proportion—the lenders are required under existing AML rules to monitor and report suspicious activity.

Beneficial Ownership

Question 60: FinCEN issued rules last May—that will come into effect in 2018—requiring banks and other financial institutions to find out the identities of people hidden behind shell companies – the so-called beneficial owners of companies. How would this rule work?

Response: On May 11, 2016, FinCEN issued the final rule on Customer Due Diligence Requirements for Financial Institutions ("CDD Rule") under the Bank Secrecy Act to clarify and strengthen customer due diligence requirements for covered financial institutions. Covered financial institutions are defined as federally regulated banks and credit unions, brokers or dealers in securities, mutual funds, futures commission merchants, and introducing brokers in commodities. The Rule imposes customer due diligence requirements on covered financial institutions that include the obligations to request the identity of beneficial owners, as defined under the Rule, from their customers and to verify the identity of those beneficial owners, subject to certain exclusions and exemptions.

Under the Rule, "beneficial owners" include any natural person that directly or indirectly holds a 25% equity interest in the legal entity customer, as well as an individual that controls the day-to-day operations of the legal entity customer. Financial institutions may rely on the representations of their customers without conducting further due diligence, unless they have reason to believe the information provided is inaccurate or unreliable. The designated legal entity customers include entities that can be described as "shell companies" due to their complex or anonymous corporate ownership structures. The CDD Rule became effective on July 11, 2016 and has an applicability date for mandatory compliance of May 11, 2018, at which time all covered financial institutions will be expected to be compliant.

Question 61: Aren't there legitimate business reasons that the "beneficial owners" of companies remain undisclosed? Is there a way to get such information into the hands of law enforcement but allow these legitimate privacy concerns to remain?

Response: FinCEN acknowledges that there can be legitimate reasons for beneficial owners of companies to desire limited disclosure of their ownership interest. FinCEN has not sought to make this information publicly available. FinCEN has weighed the desire to use legal entities to protect disclosure of individuals' activities against the positive advantages of a transparent financial system, and determined that national security, public safety, and the health of the national financial system benefit most from seeking greater transparency among legal entities. Clarifying and strengthening CDD requirements for U.S. financial institutions, including with respect to the identification of beneficial owners, advance the purposes of the BSA by:

1. Enhancing the availability to law enforcement, as well as to the Federal functional regulators and self-regulatory organizations, of beneficial ownership information about

legal entity customers obtained by U.S. financial institutions, which assists law enforcement financial investigations and a variety of regulatory examinations and investigations;

2. Increasing the ability of financial institutions, law enforcement, and the intelligence community to identify the assets and accounts of terrorist organizations, corrupt actors, money launderers, drug kingpins, proliferators of weapons of mass destruction, and other national security threats, which strengthens compliance with sanctions programs designed to undercut financing and support for such persons;
3. Helping financial institutions assess and mitigate risk, and comply with all existing legal requirements, including the BSA and related authorities;
4. Facilitating reporting and investigations in support of tax compliance, and advancing commitments made to foreign counterparts in connection with the provisions commonly known as the Foreign Account Tax Compliance Act;
5. Promoting consistency in implementing and enforcing CDD regulatory expectations across and within financial sectors; and
6. Advancing Treasury's broad strategy to enhance financial transparency of legal entities.

Question 62: How do these rules ensure active verification of beneficial owners on the part of the financial institutions?

Response: The CDD Rule requires the collection and verification of the beneficial owners of legal entity customers at the time a new account is established for a legal entity at a financial institution. Institutions may rely on the representations of their customers without conducting further due diligence, unless the institution has reason to believe the information supplied is inaccurate. Covered financial institutions are also required, on a risk basis, to update the beneficial ownership information previously collected that has become inaccurate or unreliable. As with other BSA requirements, during the examination process, examiners from the Federal banking agencies or self-regulatory organizations will actively monitor a financial institution's compliance with the Rule.

Question 63: How will this rule work for states that allow the formation of business entities without disclosure of a beneficial owner?

Response: Certain states may allow the formation of business entities without the disclosure of their true beneficial owners, and the CDD Rule does not cover this process. However, the CDD Rule will require all covered financial institutions to obtain from their legal entity customer the beneficial ownership information at the time of account opening, irrespective of whether the

legal entity was formed in a state, or a foreign jurisdiction, that allows anonymous formation of business entities.

Question 64: Isn't there consensus that identifying beneficial ownership should be collected and verified at the time a legal entity is formed, not necessarily through the financial institutions with which their customers do business? Does FinCEN believe that financial institutions have the same tools and qualifications as FinCEN and State at their disposal to adequately determine this information? Would FinCEN support legislation requiring this?

Response: Historically, Treasury has taken a three-pronged approach related to combating the misuse of legal entities: the first is strengthening the customer due diligence (CDD) obligations of financial institutions in the United States, including a requirement that they collect and verify the beneficial ownership information of new legal entity accountholders. The second prong is increasing the transparency of U.S. legal entities through the collection of beneficial ownership information at the time of company formation. The final prong is leveling the playing field internationally so countries are effectively implementing international beneficial ownership standards, and providing law enforcement with access to current and accurate beneficial ownership information in order to combat all forms of illicit finance. The key elements of effective CDD include: (i) identifying and verifying the identity of customers; (ii) identifying and verifying the identity of beneficial owners of legal entity customers (i.e., the natural persons who own or control legal entities); (iii) understanding the nature and purpose of customer relationships; and (iv) conducting ongoing monitoring of the aforementioned criteria. Collectively, these elements are best addressed by covered financial institutions and comprise the minimum standard of CDD, which FinCEN believes is fundamental to an effective AML program.

Beneficial ownership can, and does, fluctuate from the time at which an entity was formed. Therefore, requiring financial institutions to perform effective CDD at the time legal entity customers transact is essential to understanding who their customers are and what type of transactions they conduct. This is a critical aspect of combating all forms of illicit financial activity, from terrorist financing and sanctions evasion to more traditional financial crimes, including money laundering, fraud, and tax evasion.

Forming a company in the United States provides another key point of access to the international financial system. As demonstrated through the Panama Papers, companies formed in one jurisdiction may bank in a different jurisdiction. For example, a person can form a company abroad and use that company to open a bank account in the United States, or a person can form a company in the United States and use the company to open an account abroad. Therefore, it is

critical to have beneficial ownership information collected at both the time an account is opened and when a company is formed.

FinCEN does not collect beneficial ownership information, except on a case by case basis through a request for such information from a third party (i.e. a private sector vendor of such information or public sector partners through information sharing). Although FinCEN and financial institutions may have different tools, compliance with the CDD Rule does not require covered financial institutions to have or use additional tools beyond those already required to maintain compliance under the Customer Identification Program Rule.

FinCEN welcomes the opportunity to work with the Congress on any additional measures that will increase transparency into shell corporations.

Question 65: Does FinCEN currently use any other databases to find or investigate beneficial ownership?

Response: Yes, and we continually assess additional tools for obtaining beneficial ownership information.

Financial Intelligence Unit (FIU)

Question 66: How active is FinCEN currently in international training and technical assistance to foreign financial intelligence units (FIUs)?

Response: For the U.S. government, Treasury's Office of Technical Assistance (OTA) has the lead in providing anti-money laundering/countering the financing of terrorism (AML/CFT) technical assistance and training for FIUs. FinCEN and OTA collaborate on FIU issues. FinCEN provides to FIUs operational support, including analytical exchanges and workshops, as well as wide-ranging assistance to FIUs within the Egmont Group framework. As part of the Egmont Group, FinCEN carries out broad initiatives that help develop principles and best practices for FIUs and help advance FinCEN's strategic and operational objectives. For example, FinCEN proactively engages with FIUs in strategically important jurisdictions to discuss best practices and develop joint analytic projects. FinCEN engages bilaterally and multilaterally in best practices discussions with other FIUs and in operational engagements (e.g., exchange and analysis of financial intelligence regarding priority topics). FinCEN also mentors some FIUs as part of candidate FIUs' application for membership in the Egmont Group.

Question 67: Has FinCEN clarified how Treasury's Office of Technical Assistance (OTA) can best provide assistance to countries developing FIUs? How actively is FinCEN cooperating with the IMF and World Bank on such technical assistance for AML and CFT?

Response: FinCEN coordinates closely with OTA primarily when OTA is providing training and technical assistance to FIUs of strategic interest for FinCEN. FinCEN does work closely with OTA in determining how OTA can most effectively target its resources so that developing FIUs receive the training that is most necessary to promote the strengthening of a jurisdiction's AML/CFT regime. Previously, FinCEN had coordinated with donor agencies, including the IMF and World Bank, through their participation in the Egmont Group's Training Working Group. However, the last two years, FinCEN has devoted its efforts to help establish an Egmont training center to address technical assistance and training issues of FIUs and coordination with donor agencies.

Question 68: Does FinCEN work with any other agencies, like the State Department or the Department of Defense, to provide training or technical assistance?

Response: Although FinCEN does not directly engage in the provision of training or technical assistance, we do regularly work with U.S. agencies such as the State Department's Bureau of International and Narcotics and Law Enforcement Affairs and U.S. Department of Justice's Office of Overseas Prosecutorial Development Assistance and Training (OPDAT) in the provision of AML/CFT-related training and technical assistance programs.

Question 69: Can you talk about FinCEN's partnership and contribution to the Egmont Group?

Response: The Egmont Group of FIU's ("Egmont Group") provides a critical forum for FinCEN to actively promote information sharing and FIU best practices to support U.S. government AML/CFT priorities. Since the beginning of the Egmont Group in 1995, FinCEN has taken a leading role by helping to run the organization, shape the organization's strategic vision, set operational policy objectives, encourage FIUs to improve their capabilities and actively share information with partner FIUs to address priority threats. FinCEN also administers the secure network through which member FIUs communicate. FinCEN provides leadership in major Egmont Group projects aimed at sharing information to identify illicit actors and typologies related to terrorist financing, money laundering and other illicit financial activities. For example, FinCEN co-leads the Egmont Group's ISIL project that focuses on sharing strategic and tactical information to develop financial typologies and identification of previously unknown foreign terrorist fighters and their networks. The findings of this project have been shared with law enforcement and other parts of government, other 150-plus FIU members of the Egmont Group, the Financial Action Task Force (FATF), and financial sectors. The project's improved multilateral information sharing enabled FinCEN and partner FIUs, in collaboration with law enforcement and others, to identify unknown foreign terrorist fighters and their financial facilitation networks leading to multiple sanctions listings, prosecutions, sharing of relevant information before terrorist attacks, and listings on national terrorist watchlists. In addition,

FinCEN also co-leads an Egmont Group Business Email Compromise project team to analyze and target networks defrauding businesses in the United States. Since October 2014, FinCEN, in partnership with U.S. law enforcement agencies, Egmont Group FIUs, and financial institutions, has successfully recovered over $290 million for U.S. businesses.

Question 70: Are countries such as Russia contributing as much as they are benefiting from membership in The Egmont Group?

Response: Egmont member FIUs differ greatly in their legal and technical capabilities and resourcing, which impacts their ability to contribute to global anti-money laundering and countering the financing of terrorism efforts. The United States, Canada, New Zealand, and Australia are the most active FIU contributors to Egmont. The Russian FIU is also a very active Egmont member.

Question 71: How does FinCEN interact with Russia? What sorts of information are passed to Russia?

Response: As with other foreign FIUs, FinCEN has, on a limited basis, interacted and shared information with the Russian FIU under the auspices of the Egmont Group and information sharing principles. If FinCEN responds to Egmont requests by the Russian FIU for financial intelligence on a specific subject or entity that is suspected of conducting or facilitating a criminal activity in Russia, FinCEN de-conflicts responses with U.S. law enforcement agencies and other agencies as appropriate. Russia's FIU provides financial intelligence and law enforcement information in response to FinCEN and U.S. law enforcement requests for information.

Question 72: China is seeking membership in The Egmont Group. What are the criteria to joining The Egmont Group?

Response: In general, the admission of an FIU as a member of the Egmont Group is subject to the recognition that an applicant meets the definition of "FIU" and fulfils the requirements as set out in the Egmont standards. Specifically, the following requisite criteria delineate the general requirements for membership consideration:

- There should be only one entity acting as FIU in the jurisdiction, namely, receiving suspicious transaction reports and other relevant disclosures, analyzing the information, disseminating the results of the analysis, and exchanging information with the FIUs of other countries;
- Money laundering should be criminalized in line with the FATF standards;
- Terrorist financing should be criminalized in line with the FATF standards;

- Financial Institutions and Designated Non-Financial Businesses and Professions should be obliged to report suspicions promptly to the FIU when they suspect or have reasonable grounds to suspect that funds are the proceeds of a criminal activity, or are related to terrorist financing, in line with the FATF standards.
- The FIU should be operationally independent and autonomous in performing its functions of receipt, analysis and dissemination, in making use of the powers available to perform these functions, in carrying out international cooperation;
- The FIU must have the authority and capacity to request information from reporting entities and other sources;
- The FIU should conduct operational and strategic analysis;
- The FIU should have access to the widest possible range of financial, administrative, and law enforcement information;
- The FIU should exchange information freely, spontaneously and upon request, on the basis of reciprocity; and
- The FIU should rapidly, constructively and effectively provide the widest range of International cooperation to counter money laundering, associated predicate offence and the financing of terrorism.

Question 73: Does FinCEN support China's Egmont membership? How?

Response: FinCEN and the FIU of Spain are co-sponsoring the membership application of the Chinese FIU to the Egmont Group. FinCEN has sent teams of experts to visit China's FIU and their FIU has visited FinCEN to consult on the Egmont membership process and FIU best practices and policies. FinCEN has collaborated closely with the State Department and our Treasury Department colleagues on US-China foreign policy issues. FinCEN and the Chinese FIU also exchange financial intelligence on a variety of cases pursuant to an MOU.

Information Sharing

Question 74: How does FinCEN share its analysis with its counterparts?

Response: FinCEN regularly presents the findings of its analysis at conferences and briefings throughout the country and in international fora such as the biannual Egmont Plenary. FinCEN disseminates these products to a broad list of customers through a number of mechanisms: via encrypted email; through a searchable repository available to all 11,000 users of the FinCEN portal; via the Egmont Secure Web to our 156 international partner FIUs; and via a FinCEN special interest group on the FBI's LEEP. FinCEN also works closely with Treasury's intelligence community component, the OIA, to disseminate information from select BSA reports to our national security partners via classified networks. We currently share our products with federal law enforcement agencies and inspectors general; several state, local, and tribal law

enforcement organizations; the U.S. intelligence community; our international law enforcement partners, and certain foreign regulatory counterparts.

Question 75: How does FinCEN determine which counterparts with whom to share? Does FinCEN share every analytic product with everyone?

Response: We target the distribution of our analytical products to the appropriate agencies. In general, FinCEN has customized email distribution lists for different sets of customers. These are typically topic-based, such as cyber or counterterrorism. For products posted to the FinCEN portal, we separate our recipient audiences based on whether or not they are a law enforcement or regulatory partner.

Question 76: How does FinCEN gather feedback on its products? What sorts of feedback does FinCEN get, and how does it receive that feedback?

Response: FinCEN solicits feedback on its products via both explicit (electronic feedback forms and surveys) and implicit (product views and downloads) mechanisms. FinCEN use a variety of data collection methods. These methods include online feedback surveys, as well as meeting with representatives from both domestic law enforcement and foreign FIUs. Feedback is also collected from stakeholders via feedback forms that are included with FinCEN products, as well as email correspondence and formal HUMINT Online Tasking and Report evaluations of our Intelligence Information Reports (IIR) shared through classified channels.

Question 77: How does FinCEN share its analysis with foreign partners?

Response: FinCEN shares its analysis with foreign FIU partners via the Egmont Secure Web.

Question 78: Does FinCEN share only with other FIUs, or does it share with non-FIU foreign counterparts, like law enforcement agencies, intelligence authorities, and regulators?

Response: Besides our FIU partners, FinCEN also shares our analytical products with federal law enforcement and regulatory agencies and inspectors general; several state, local, and tribal law enforcement organizations; the U.S. intelligence community; international law enforcement partners, and certain foreign regulatory counterparts.

Question 79: Can you describe how you are currently expanding your dissemination system to move away from point to point delivery?

Response: FinCEN is currently in the middle of posting all of our financial intelligence products and Flash reports to the FinCEN portal in order to facilitate access to all 11,000 portal users. We are also posting a limited number of products to a classified SharePoint portal for our intelligence and law enforcement customers.

Question 80: How does FinCEN disseminate its classified products?

Response: FinCEN disseminates its classified products via a SharePoint portal, classified email, and through the joint program with OIA to create IIRs. The IIR program produced 567 IIRs in FY17. These reports provide FinCEN's national security stakeholders with unique financial intelligence in a format that can be readily indexed and searched by U.S. national security systems.

Questions for the Record for FinCEN Acting Director Jamal El-Hindi
House Committee on Financial Services
Hearing before the Subcommittee on Terrorism and Illicit Finance entitled
"Safeguarding the Financial System from Terrorist Financing"
Thursday, April 27, 2017

Questions for the Record Submission from Representative French Hill (AR-2)

Question 1: During the hearing, you agreed to provide a memo describing unfilled vacancies and hiring challenges at FinCEN. Please ensure that the memo describes:

- The number of vacancies compared to authorized FTEs for each of the last five Federal fiscal years, and a general description of the types of vacancies (e.g., analyst, support, etc.).
- The number of positions assigned to each FinCEN division, including the number of positions in each division that are filled, that are currently unfilled but with job offers made, and the number that are unfilled and awaiting further action.
- The reasons such spots were unfilled.
- The average length a position was vacant, the extent to which security clearance investigations contributed to vacancies, and what other structural problems contributed to vacancies.
- The average length of time to fill a vacancy, starting from initial vacancy (because of the creation of the position, departure of an employee, etc.) to the entry on duty of an employee hired to fill that billet.
- The yearly attrition rate of FinCEN employees for any reason, including retirement, change of employment, etc.
- The process by which FinCEN prioritizes which vacancies to hire first, and the reasons or strategy used to justify prioritizing one position over another.
- The current process FinCEN uses to hire a new employee, including classification of a position, advertising of a position, interviewing, offering a job, background and clearance investigation, and onboarding the employee.
- The steps being taken to speed up hiring.
- Any current or proposed recruitment, hiring, and retention strategies (if any) designed to address the gap in FinCEN personnel.
- The anticipated amount of time FinCEN believes necessary to fill all existing vacancies.
- The number of personnel in the Human Resources office, including the number of personnel dedicated to processing and filling job vacancies.
- The effect on FinCEN's mission of having so many vacancies.

- The amount of funding provided by Congress for FTE salaries that was unused for such salaries because of these vacancies.
- The uses to which funding for such vacancies was put (e.g., returned to Treasury, used for other purposes and if so which purposes)
- Why FinCEN did not bring the number of vacancies to Congressional attention.
- Any legislative steps necessary to correct problems that have slowed the hiring process. Such as giving FinCEN "fast track" authority for hiring analysts, such as other elements of the intelligence community.

Response:

INFORMATION MEMORANDUM FOR REPRESENTATIVE FRENCH HILL

FROM: Jamal El-Hindi, Acting Director

SUBJECT: FinCEN Vacancies and Hiring Challenges

This is in response to your questions about FinCEN hiring during my testimony before the Subcommittee on Terrorism and Illicit Finance on April 27, 2017 and your subsequent Questions for the Record.

The following chart shows FinCEN's Full Time Equivalents (FTE) targets that were included in the President's budget requests to Congress, the FTE targets included in the appropriations bills enacted by Congress, actual FTE, new hires, employee departures, and FinCEN's attrition rate for the past six years.

FinCEN Full Time Equivalents (FTE), Average On-Board, and Attrition Rate

	FY 2012	FY 2013	FY 2014	FY 2015	FY 2016	FY 2017
FTE Funded in President's Budget	304	322	340	345	343	343
FTE in Enacted Level	327	341	345	345	343	343
Actual FTE	299	300	279	275	278	274
New Hires	35	21	23	36	26	20
Employee Departures	-31	-38	-34	-36	-29	-25
Attrition Rate	10.3%	12.6%	12%	13%	10.4%	9.1%

FinCEN has had a high number of vacancies over the past five years. A number of factors have contributed to these vacancies, including FinCEN's controlling hiring to meet the lower FTE target in the President's budget in 2012-2013, implementation of a major reorganization in 2013-

2014, a substantial number of internal hires, promotions, and reassignments, and significant delays in background investigation processing at the Office of Personnel Management. FinCEN's attrition rate has also been consistently higher than the government-wide rate of around 6%, adding to FinCEN's staffing issues, as it takes significantly more time to clear and onboard new personnel than it takes for an employee to submit his or her resignation and depart from the organization. The timeframe for actual onboarding varies from weeks to over a year and is largely dependent upon factors outside of FinCEN's control (e.g. candidate's clearance status and OPM background investigation process and backlog).

Since my testimony on April 27, 2017, FinCEN has on-boarded 51 new personnel and promoted/reassigned 30 FinCEN employees. This progress was offset, however, by 52 separations and the 30 additional vacancies created by the internal moves, leaving FinCEN with 58 current vacant positions. Of these 58 positions, 16 are in the early stages of recruitment (e.g. position analysis and classification), and all vacancies identified in the TFI-approved hiring surge initiated on January 8, 2018, are on track to be posted to USAJobs by June 15, 2018. When filling vacancies, FinCEN focuses priority attention on key leadership positions and those positions most critical to accomplishing FinCEN's mission. Currently these priorities are in the Enforcement, Policy, Management, and Liaison Divisions. With few exceptions, FinCEN positions are filled using the competitive procedures outlined in Title 5 of the Code of Federal Regulations. To help speed the part of the recruitment process that FinCEN can control, the Human Resources Office has worked directly with supervisors in the recruitment process and has used contract employees to support position classification and development of evaluation questions, crediting plans, and other recruitment materials. FinCEN is also using the Bureau of Fiscal Services' Administrative Resource Center to issue vacancy announcements and evaluate qualified candidates. These contracts help augment FinCEN's two Human Resources FTEs.

FinCEN completed the Office of the Director of National Intelligence-directed position review and designation activity in July 2017. As a result, 17 positions were reduced from Top Secret (requiring an average of 335 days for OPM background investigation) to Secret (requiring 107 days) or Public Trust (requiring 165 days), and two Secret positions were reduced to Public Trust, thereby reducing the amount of time required to recruit and hire personnel into these positions in the future. (For reference, it takes about 100 days from the start of the staffing process to the tentative offer that initiates the background investigation process.)

FinCEN's current vacancies as of May 7, 2018, are shown by division in the following chart.

Division	FTE Target	On-Board	Vacant	Pending EOD	Pending Background Invest.	Recruitment	Pre-Recruitment	Positions

Office of Director	15	16*	0	0	0	0	0	FinCEN Director
Chief Counsel	14	12	2	0	1	0	1	Attorney Advisors
Technology	39	28	11	1	1	5	4	Information Technology Specialists
Management	43	34	9	0	2	6	1	Human Resources, Financial Management, and FOIA Specialists
Intelligence	85	74	11	1	7	2	1	Intelligence Research Specialists
Enforcement	52	40	13*	0	3	5	5	Enforcement Specialists
Policy	27	22	5	0	1	2	2	Regulatory and Strategic Policy Specialists
Liaison	65	60	5		1	2	2	Liaison and Case Management Specialists, Editors
Total	340	286	56	2	16	22	16	

**FinCEN manages to projected vacancies, creating an appearance of discrepancy in "Onboard" and "Vacant" numbers.*

All funding provided to FinCEN is used to meet a growing critical national security mission and to ensure continued focus and analysis on new and existing threats to the financial system. Although the workforce is not at full strength, FinCEN uses funding for a variety of support contracts that enable the Bureau to leverage the federal workforce to meet the growing demand for FinCEN data and to address emerging threats to the financial system. These contracts provide case support and functional specialists, cyber security experts to respond to the expanding cyber threat, human resources expertise to support critical hiring priorities, and data analysts and expertise to support financial intelligence analysis.

Question 2: FinCEN intelligence analyst positions are not "excepted," which especially in view of other hiring issues would seem to put FinCEN at a particular disadvantage should an analyst leave. What is the average tenure of an intelligence investigator at FinCEN?

a. **What steps would be necessary to "except" those positions—must that be done legislatively or could that be done by the Treasury Department Secretary or Under Secretary? Are there other analytic positions that are essential enough that they ought to be excepted as well? Please elaborate.**

Response: The average tenure of a FinCEN's intelligence research specialists is 16.1 years (compared to an overall tenure of 14.8 years for all FinCEN employees). FinCEN would welcome any opportunity to explore expanding our hiring authorities. If FinCEN were to be granted excepted service hiring authority, it would allow us to compete for talent the same way as many of our excepted service agency counterparts do. For example, we could increase our diversity of skillsets and backgrounds. We would be open to working with this Committee on any proposal you may have.

Question 3: You said FinCEN has job-retention tools available to help hold onto top-quality staff who might be tempted by other jobs. Please describe the range of tools available, how they compare to other Federal agencies with retention tools (bonuses, pay surcharges, over-scale payments, etc.), and specifically how they have been used in each of the last five years, including the frequency of use, the process for determining when to use the retention tools, the reasons used to justify the use of the tools, and the effectiveness of the tools, such as the numbers of employees actually retained because of the tools' use. Also, please inquire with division heads for their impressions about whether the retention tools are adequate and adequately used, or whether they believe they have lost staff because such tools are inadequate or not used enough.

Response: Similar to other Federal agencies, FinCEN has the authority to pay recruitment and relocation bonuses for hard-to-fill positions. FinCEN also may hire an employee at a higher rate of pay if he or she has superior qualifications. However, FinCEN's challenge is generally not in attracting qualified candidates; most vacancy announcements receive a significant number of well-qualified applicants. FinCEN does have—and utilizes—authority to pay employees a retention bonus. FinCEN uses this mechanism rarely, however, as it only applies when the employee receives a bona fide job offer in the private sector. (Employees leaving to pursue a higher paying job in another Federal agency are not eligible for retention bonuses).
In lieu of financial incentives, FinCEN has focused attention recently on improving employee morale and engagement as a means to improve retention and to reduce the attrition rate. In particular, FinCEN established an employee-led group to define a desired culture for the organization and lead efforts to reach that desired state. FinCEN has also taken steps to enhance the onboarding experience and improve the start of its relationship with new employees.

"Safeguarding the Financial System from Terrorist Financing"
Thursday, April 27, 2017

Questions for the Record Submission from Representative Mia Love (UT-4)

Question 1: How does FinCEN choose its business rules?

Response: FinCEN employs automated business rules to combat our most significant money laundering and terrorist financing threats. The rules are developed using subject matter expertise and information collected from FinCEN analysts, law enforcement partners, and external stakeholders. The rules align with FinCEN's six priority areas including transnational security threats, cybercrime, transnational organized crime, significant fraud, compromised financial institutions, and third party money launderers.

Question 2: Who approves or disapproves new business rules, and what criteria are used to judge the suitability of a particular rule?

Response: FinCEN has a business rules management team that oversees the design, development and implementation of all new business rules. All requests for new rules are submitted via an application process. Applications are reviewed by the business rules management team to ensure the rule aligns with FinCEN priorities. Once approved, the application is then reviewed by FinCEN Counsel to ensure the rule does not violate the privacy or civil liberties of United States citizens. Once the rule has been approved by the management team and FinCEN Counsel, the rule development team conducts an impact assessment to ensure the rule will perform within accepted standards and not capture excessive volumes of information not relevant to the rule's intended purpose.

Question 3: Are rules ever retired from use? If so, why?

Response: FinCEN conducts a 45-day efficacy assessment of all new rules deployed in our production environment to ensure the rule is performing within accepted standards and is not capturing excessive volumes of information not relevant to the rule's intended purpose. If the rule is capturing an excessive volume of information or is not performing within accepted standards, the rule is modified or retired. If the rule is modified, it will be re-evaluated again after six months to ensure the rule's performance has improved.

All existing business rules are continually monitored for efficacy (both quantitative and qualitative) and each undergoes a formal bi-annual review and certification process. If the rule is not performing within acceptable standards, then it is retired.

Question 4: How many rules are currently run?

Response: Since 2014, FinCEN has deployed 95 business rules. Currently, there are 62 active business rules.

Question 5: How frequently are the business rules run? Are they real-time?

Response: FinCEN's business rules are run on a daily basis against all incoming Bank Secrecy Act (BSA) data.

Question 6: What are the search terms for these particular rules?

Response: FinCEN's business rules range in complexity from traditional "watch list" rules designed to identify known illicit actors to complex multi-variable weighted rule sets capable of identifying emerging illicit activity. The rules search the BSA filings for key terms, entities, and typologies.

Question 7: What subjects or topic areas are currently the subjects of business rules?

Response: FinCEN's business rules align with the organization's six priority areas including transnational security threats, cybercrime, transnational organized crime, significant fraud, compromised financial institutions and third party money launderers.

Question 8: How frequently are the business rules updated or changed with new terms or methodologies?

Response: FinCEN updates business rules on a weekly deployment/release cycle. For national security issues or in emergency situations, FinCEN has the ability to update and/or deploy new rules within 24 hours.

Question 9: How frequently are the business rules run? Are they real-time?

Response: FinCEN's business rules are run on a daily basis against all incoming BSA data.

Question 10: What output do the business rules provide?

Response: FinCEN's business rules produce more than 5,000 rule findings per month. The rule findings point FinCEN analysts to specific filings for hands-on review and focus their efforts on the filings most likely to be key in defending against priority threats.

Question 11: How are the business rules evaluated for effectiveness?

Response: FinCEN conducts a 45-day efficacy assessment of all new rules deployed in our production environment to ensure the rule is performing within accepted standards and is not capturing excessive volumes of information not relevant to the rule's intended purpose. If the rule is capturing an excessive volume of information or is not performing within accepted standards, the rule is modified or retired. If the rule is modified, it will be re-evaluated again after six months to ensure the rule's performance has improved. All existing business rules are continually monitored for efficacy (both quantitative and qualitative) and each undergoes a formal bi-annual review and certification process. If the rule is not performing within acceptable standards, then it is retired.

Question 12: Do these rules inform Flash Reports?

Response: FinCEN has a number of business rules designed to identify illicit financial activity associated with both domestic and international terrorism. These rules form the basis for FinCEN's Intelligence Flash Reports. Output from the rules is screened on a daily basis and the most valuable information is selected for inclusion in FinCEN's Flash Reports.

Question 13: How are these reports utilized? Who utilizes them?

Response: Flash Reports provide critical financial intelligence to FinCEN's domestic law enforcement stakeholders, the Intelligence Community, and Financial Intelligence Unit (FIU) partners around the world. Terrorist financing-related Flash Reports assist law enforcement efforts aimed at cutting off terrorist groups' sources of revenue, preventing terrorist groups' access to the international financial system, identifying unknown foreign terrorist fighters, and identifying information related to known actors. The Flash Reports direct law enforcement's attention to particular reporting in the database. The reports are provided for financial intelligence purposes to alert about possible threats and to assist in ongoing investigations.

Question 14: How is all of this information processed and communicated to law enforcement authorities?

Response: FinCEN communicates the financial intelligence it receives by: (1) providing both direct access to the BSA filings it receives and (2) creating a variety of finished products for our federal, state, local, tribal, and foreign law enforcement partners. These law enforcement partners receive FinCEN products ranging from brief reports on filings of note to strategic analyses of illicit financing methodologies through various mechanisms: encrypted email; through a searchable repository on the FinCEN portal; and a FinCEN special interest group on

the FBI's Law Enforcement Enterprise Portal. FinCEN also works closely with Treasury's intelligence community component, the Office of Intelligence and Analysis, to disseminate select BSA reports to law enforcement partners via classified networks. Finally, FinCEN oversees the receipt and processing of several thousands of requests for information and information exchanges in support of our law enforcement, regulatory, national security, and international partners (i.e., foreign FIUs) via the Egmont Secure Web annually.

Question 15: How many "queries" or requests for information does FinCEN staff handle each day?

Response: In FY 2017, FinCEN received:

- 1,017 (3.9 per day) Requests for Information from Egmont FIU partners
- 1,142 (4.4 per day) Spontaneous Disclosures of Information from Egmont FIU partners
- 1,882 (7.2 per day) Requests for Suspicious Transaction Report Supporting Documents from U.S. Requesters (e.g., law enforcement, regulators, FinCEN) and Egmont FIU Partners
- 413 (1.6 per day) Requests from U.S. Requesters to Egmont FIU partners
- 396 (1.5 per day) 314(a) requests
- 38 (2 per day) Requests for BSA Certified Records
- 18,130 (69 per day) Regulatory Guidance Inquiries

Question 16: How do outside agencies, like the U.S. Customs and Border Patrol (CBP) or the Federal Bureau of Investigation (FBI), utilize Flash Reports?

Response: Flash Reports are one method by which FinCEN proactively disseminates BSA analysis to our partners. These reports are intended to serve as lead information for our partners, including CBP and FBI.

Question 17: Can outside agencies submit business rules to FinCEN for use?

Response: FinCEN currently operates business rules for external stakeholders on a very limited basis.

Question 18: Do outside agencies receive the output of the business rules?

Response: The business rules are automated queries or algorithms applied to BSA data to identify records of interest and point FinCEN analysts to specific filings for hands-on review. This helps analysts examine and exploit large volumes of BSA data and enables more complex

search capabilities. The output of these business rules are reviewed by analysts and often turned into analytical products that are shared with relevant stakeholders.

Question 19: Please provide an example of a business rule and a product produced from the results of a business rule.

Response: FinCEN continually leverages automated rules in the fight against Islamic State in Iraq and Syria (ISIS). FinCEN has employed fifteen rules pertaining to ISIS and its activities. These rules are instrumental in producing an important stream of timely financial intelligence on ISIS for FinCEN analysts and external stakeholders. In addition to the Intelligence Flash Reports FinCEN has developed from our ISIS business rules, FinCEN also uses the output from business rules to develop Executive Alerts, Intelligence Assessments, and Targeting Reports.

Questions for the Record for FinCEN Acting Director Jamal El-Hindi
House Committee on Financial Services
Hearing before the Subcommittee on Terrorism and Illicit Finance entitled
"Safeguarding the Financial System from Terrorist Financing"
Thursday, April 27, 2017

Questions for the Record from Representative Luke Messer (IN-6)

Question 1: There is a viewpoint that FinCEN gets "too much" information and thus is unable to sort through it for important indicators of crimes. Could you please address that?

a. Is FinCEN concerned with the number of SARs filed or the quality of SARs filed?

Response: FinCEN focuses on the quality of CTRs and SARs filed by an institution. We expect financial institutions to fulfill their regulatory requirements and file the appropriate BSA forms accurately and completely as part of an overall risk based approach. There is no quota system or regulatory expectation regarding how many CTRs and SARs an institution "should be filing." Moreover, FinCEN has studied the issue of "defensive filing" by reviewing samples of SAR filings and has found little evidence of unnecessary SAR filings. To the contrary, FinCEN believes financial institutions are doing a good job of spotting and reporting suspicious activity that is of high-value to law enforcement. It is worth noting that the value of reporting suspicious activity is multiplied when many financial institutions are watching for, and sharing information on, similar activity. What, in isolation, seems to be a minor report from one institution may, in fact, be illustrative of a broad and dangerous trend when viewed in context of other filings.

While it is true that the volume of this information has increased, so has our capacity to extract valuable information. Through the use of algorithms, and the alertness of financial institutions, we are now able to identify flows or funds and persons related to potential foreign terrorist fighters that otherwise would have gone unnoticed a decade ago. In studying those patterns, we are also seeing terrorist organizations resorting to more common illicit activity to generate funds or hide them. We are always looking for ways to improve our system and are always interested in the thoughts that industry and law enforcement have on ways to make the system more effective.

Question 2: How active is FinCEN current in international training and technical assistance to foreign financial intelligence units (FIUs)?

a. Does FinCEN work with any other agencies, like the State Department or the Department of Defense, to provide training or technical assistance?

Response: For the U.S. government, Treasury Department's OTA has the lead in providing AML/CFT technical assistance and training for FIUs. FinCEN and OTA collaborate on FIU issues. FinCEN provides to FIUs operational support, including analytical exchanges and workshops, as well as wide-ranging assistance to FIUs within the Egmont Group framework. As part of the Egmont Group, FinCEN carries out broad initiatives that help develop principles and best practices for FIUs and help advance FinCEN's strategic and operational objectives. For example, FinCEN proactively engages with FIUs in strategically important jurisdictions to discuss best practices and develop joint analytic projects. FinCEN engages bilaterally and multilaterally in best practices discussions with other FIUs and in operational engagements (e.g., exchange and analysis of financial intelligence regarding priority topics). FinCEN also mentors some FIUs as part of candidate FIUs' application for membership in the Egmont Group.

Although FinCEN does not directly engage in the provision of training or technical assistance, we do regularly work with U.S. agencies such as the State Department's Bureau of International and Narcotics and Law Enforcement Affairs and U.S. Department of Justice's OPDAT in the provision of AML/CFT-related training and technical assistance programs.

Question 3: How does FinCEN share its analysis with its counterparts?

Response: FinCEN shares products and analysis with federal law enforcement agencies and inspectors general; several state, local, and tribal law enforcement organizations; the U.S. intelligence community; and international partners. FinCEN disseminates its products to this broad list of customers through a number of mechanisms: (1) encrypted email; (2) a searchable repository available to all 11,000 users of the FinCEN portal; (3) the ESW to our 156 international partner FIUs within the Egmont Group; and the FBI's Law Enforcement Enterprise Portal to a FinCEN special interest group. FinCEN also works closely with Treasury's intelligence community component, the Office of Intelligence and Analysis, to disseminate information from select BSA reports to our national security partners via classified networks.

Question 4: How does FinCEN determine which counterparts with whom to share? Does FinCEN share every analytic product with everyone?

Response: FinCEN does not share every analytic product with everyone. In general, FinCEN has customized email distribution lists for different sets of customers. These are typically topic-based, such as cyber or counterterrorism. For products posted to the FinCEN portal, we separate our recipients based on whether or not they are a law enforcement or regulatory partner.

Question 5: How does FinCEN share its analysis with foreign partners?

Response: FinCEN shares its analysis with foreign partners via the ESW, particularly, if there is suspicion of a crime in that partner's jurisdiction or if we believe that a jurisdiction may have information that may forward one of our own investigations. In addition, FinCEN shares information about suspected terrorism or terrorist financing broadly with select partner FIUs regardless of whether there is a direct link with the jurisdiction; FinCEN recognizes that when FIUs work multilaterally to share their information, they are more effective at shining light on potential criminal subjects and suspected illicit networks. FinCEN co-led an important analytical project in the Egmont Group on countering financing related to foreign terrorist fighters (FTFs) and ISIL by assembling a coalition of FIUs for more than two years. The results of the multilateral information sharing led to the detection of suspected FTF subjects, an identification of indicators of FTF financing and a recognition of challenges that FIUs are having in CFT.

Question 6: In March 2015, Italy, Saudi Arabia, and the United States launched the first meeting of the Counter-ISIL Finance Group. Now that almost two years has since passed, what early lessons can be gleaned from the U.S. and international response to combating Islamic State finances? Where were the early policy obstacles? What was needed to overcome them? What would have improved outcomes and hastened response times?

Response: The Counter ISIS Finance Group (CIFG), which the United States leads with Italy and Saudi Arabia, is an integrated part of the broader Defeat ISIS Coalition. The working group is unique in that it is the only multilateral body focused exclusively on disrupting ISIS's sources of wealth and its access to the international financial system. The CIFG is made up of a diverse and knowledgeable group of 40 members and observers, including key Coalition partners and international bodies such as the Financial Action Task Force, the United Nations Monitoring Team, and the Egmont Group of financial intelligence units. As part of its ongoing work, the CIFG is focused on information exchange, the future of non-oil revenues, and ISIS's abuse of money services businesses. The CIFG has provided an important platform for member countries to highlight successes and lessons learned in combatting terrorist financing, develop coordinated countermeasures, and increase our understanding of ISIS's finances.

Questions for the Record for FinCEN Acting Director Jamal El-Hindi
House Committee on Financial Services
Hearing before the Subcommittee on Terrorism and Illicit Finance entitled
"Safeguarding the Financial System from Terrorist Financing"
Thursday, April 27, 2017

Questions for the Record from Representative Robert Pittenger (NC-9)

Question 1: Can you please provide examples of how law enforcement uses BSA data? Specifically, please provide examples of BSA data that has led to arrests, prosecutions, and/or convictions.

Response: In 2015, FinCEN began recognizing law enforcement agencies that effectively used BSA data to obtain a successful prosecution, and to provide concrete evidence of the value of BSA data to the reporting financial industry. Below are the summaries of the award winning cases from the FinCEN's 2017 Law Enforcement Awards:

(1) SAR Review Task Force: New York State Police

The New York State Police Special Investigations Unit at the Financial Crimes Unit identified suspicious transactions occurring in the Hudson Valley Region indicative of money laundering as part of SAR review initiatives. The impetus of the investigation was a single financial institution reporting an unusual pattern of cash deposits. The reporting bank indicated that it believed much of the cash was derived from the illegal sale of marijuana. The funds were rapidly withdrawn from ATM locations across the United States. Investigators identified many additional reports containing sensitive financial information, dating back another year, indicating similar activity in this account.

Further investigation demonstrated that these individuals were connected to a larger criminal organization than originally believed, allowing the organization to be considered an "enterprise" and eligible to be charged under the Racketeer Influenced and Corrupt Organizations Act.

Investigators discovered extensive criminal histories for many of the individuals associated with this organization, including narcotics and firearms possession charges on several individuals. The Special Investigations Unit initiated a criminal investigation, and the two parallel investigations led to the identification of expansive criminal organizations responsible for bringing large quantities of narcotics into the region, operating business

fronts used to launder funds, weapons trafficking, bulk cash smuggling, and extensive gang activity, including murder. Over 100 individuals belonging to several different street and prison gangs were identified, ranging from leadership to low-level associates, along with residences and vehicles belonging to these individuals.

As a result of this multi-agency investigation, law enforcement successfully seized 16 firearms, 14 kilos of cocaine, 12 pounds of marijuana, 90 grams of crack cocaine, 153 grams of heroin, 75 oxycodone pills, $200,000 in cash, and several vehicles. Thirty defendants have been convicted or pleaded guilty in the Northern and Southern Districts of New York, and prosecution is ongoing for 16 others.

(2) Transnational Organized Crime: Federal Bureau of Investigation

The FBI initiated an investigation after receiving a referral from local law enforcement regarding an individual suspected of carrying out various fraud and money laundering schemes. A review of sensitive financial information identified a high volume of data enabling investigators to identify 80 accounts controlled by the primary target and identify funds that appeared to be derived from criminal activity. The individual was arrested and charged with money laundering, which subsequently led to his cooperation with law enforcement.

Based on information this individual provided after agreeing to cooperate with the FBI, investigators uncovered a network of criminal actors located in the United States and Canada. Investigators then used this information to identify additional accounts and transactions involving these newly identified targets at financial institutions located throughout the United States. These financial institutions described suspected money laundering activity though a series of businesses and trust accounts located in several countries. Investigators also identified additional ongoing criminal investigations by other agencies targeting this same network of individuals.

Investigators began working closely with the other agencies to identify the full scope of this criminal organization. The information obtained during this coordination led the FBI to consider this criminal organization one of its highest priority transnational organized crime targets. Working closely with foreign and domestic law enforcement partners, investigators identified members of this criminal organization operating from all over the world. Analysis of financial activity indicated that this organization was bringing in $100-$300 million in annual criminal proceeds in North America alone.

Authorities arrested and indicted the targets on various money laundering, fraud, and conspiracy charges. Several suspects pled guilty before their cases went to trial. Several targets went to trial, where all defendants were convicted on all counts.

(3) Transnational Security Threats: Federal Bureau of Investigation

The FBI used a high volume of sensitive financial information over several years during the course of its investigation into a criminal organization moving hundreds of millions of U.S. dollars to support foreign nuclear and ballistic missile programs.

This investigation identified two families engaged in criminal activities. These families each operated a network of exchange houses, precious metals companies, trading companies, and front companies throughout the Middle East to carry out financial activity for the benefit of multiple Office of Foreign Assets Control-sanctioned entities, as well as several entities with close ties to foreign military organizations.

This investigation utilized information gleaned from financial data to confirm information necessary to issue search warrants and subpoenas to multiple U.S. financial institutions. Piecing together many pieces of financial data, they determined that the targets were operating one particular exchange house for foreign remittances. The investigation ultimately identified millions of transactions totaling over $200 billion.

During the FBI investigation, foreign authorities took legal action against several of the targets, who were arrested on a range of charges, including billions of dollars in bribery, corruption, and embezzlement. While most of these charges were ultimately dropped, the FBI was able to compare data about the foreign law enforcement investigation with evidence it had obtained through its own investigation and determined that many significant elements of the foreign investigation supported conclusions the FBI had drawn based on email, bank, and other data. As a result of the publicity generated by the foreign investigation, law enforcement gathered additional and previously unknown details on the identified individual targets and their hundreds of associated shell companies. This allowed the FBI to expand its search and more completely map out the criminal network and its funding mechanisms.

The investigation ultimately led to criminal charges of bank fraud, money laundering, and conspiracy to commit money laundering, bank fraud, and sanctions violations through two separate indictments against 13 individuals. Prosecution of these individuals is ongoing. Criminal forfeiture totals are expected to reach hundreds of millions of dollars.

(4) Cyber Threats: Internal Revenue Service-Criminal Investigation

A multi-year, multi-agency investigation, led by IRS-CI focused on several targets selling narcotics on the dark web and distributing them throughout the United States through the U.S. Postal Service. The primary targets of this investigation conducted their online activity through The Onion Router which provided them with encryption and decryption of peer-to-peer connections. This method provided the targets with access to several dark web sites, on which they sold methamphetamine and marijuana.

The targets disguised their shipments of narcotics through the Postal Service inside packages filled with markers and drawing paper. Despite the targets' use of multiple return addresses and sender names, Postal inspectors were able to determine that the suspected narcotics mailings were originating from the same individuals based on several telling packaging characteristics.

Investigators intercepted multiple packages as a result of search warrants. Investigators were then able to determine through internet service provider records that the username associated with several undercover purchases on the dark web belonged to the same individual sending the narcotics through the Postal Service. Investigators determined that over a 6-month period, this individual sent 435 suspicious packages on at least 50 different occasions.

Sensitive financial information identified during the course of this investigation detailed specific information that corroborated the financial and personal information of the subjects of the investigation. The data also indicated that the subjects were using Bitcoins in an effort to conceal their illicit proceeds. The information identified in the financial data and from subpoenas issued to numerous financial institutions and Bitcoin exchangers helped clarify the convoluted series of transactions conducted to launder the funds.

The targets only accepted payment for the narcotics in the form of Bitcoin. The Bitcoins were then sent through a Bitcoin "blender" to conceal their source. The Bitcoins would then be redistributed back to the targets through several Bitcoin exchangers before being converted into U.S. dollars and deposited into several bank accounts.

The targets of this investigation were arrested on various drug charges, at which point several search warrants were issued on several locations where methamphetamine, marijuana, and numerous firearms were discovered. The targets were subsequently indicted and pled guilty to various drug and money laundering charges. This is notable since this is the first case in this particular Midwest district where money laundering charges were approved based on Bitcoin transactions.

(5) <u>Significant Fraud: Defense Criminal Investigative Service</u>

DCIS initiated a long-term investigation based on structuring and excessive credit card charges identified by multiple financial institutions on a single individual. Two different working groups identified the transaction data and referred it for further investigation. Investigators determined that one of the subjects was transferring funds to a company providing subcontractor support for a military contract in Afghanistan. Further investigation determined that the company receiving the funds was a shell company owned by a U.S. military official to conceal bribery payments he was receiving in exchange for helping the primary target win contracts.

Further financial analysis identified $24 million in transactions in the personal accounts of the primary target. The majority of the transactions were multi-million dollar deposits from his employer, which was a U.S. Department of Defense prime contractor providing logistical support and training to foreign military units. These deposits were followed immediately by transfers to several bank accounts and structured cash withdrawals.

A detailed analysis of sensitive financial information and contract documents revealed that the U.S. military official received bribes from the primary target in exchange for sensitive bidding data, including bid amounts of competitors and actual government estimates. The official was also responsible for establishing those estimates and assembling the team responsible for reviewing bids. In return for his assistance in winning $54 million in bids, the primary target paid the official over $9 million through an extensive network of shell companies and bank accounts.

The targets of this investigation eventually pled guilty to various conspiracy, money laundering, obstruction, and fraud charges. Investigators seized $12.3 million in assets from the primary target and his employer and the military official, including real property, vehicles, boats, aircrafts, firearms, gold coins, and bank accounts.

(6) Third-Party Money Launderers: Homeland Security Investigations

Over the course of 18 months, HSI investigators utilized an extensive volume of sensitive financial information to assist in their investigation into a large-scale illegal third-party money laundering organization. The investigation began based largely on information gleaned from a FinCEN-issued GTO. This GTO required armored car services importing or exporting funds through two specific geographies in the southwest border region to acquire additional identifying information on certain transactions.

The information that investigators discovered as a result of the GTO led them to focus on one particular armored car company that appeared to be facilitating a money laundering scheme outside southern California. Investigators discovered that the company was importing U.S.

dollars and Mexican pesos from casas de cambio in Mexico and depositing them into shell company bank accounts that were opened and operated by the two individuals who owned and operated the company.

Law enforcement was able to identify and connect an address for the armored car company that was shared by several other companies owned by the same individuals. Two of these newly identified companies were registered as MSBs. Further investigation and a detailed analysis of financial data indicated that these additional companies were simply shell companies that the two individuals used to funnel millions of U.S. dollars back into Mexico.

Subpoenas were issued to the banks used by each of these companies, as well as to all of the people known to be involved with the companies. Transaction records identified cash deposits of $45 million over a 15-month period, which were then transferred in and out of the accounts of the various companies owned by the individuals before ultimately being wired to Mexico.

As a result of the investigation and discovery of the money laundering scheme, both individuals pled guilty to violations regarding failures to maintain an effective anti-money laundering program. They also lost all licenses necessary to operate as an MSB and forfeited hundreds of thousands of U.S. dollars and Mexican pesos.

Question 2: Please articulate the importance of Patriot Act Section 314(a) and (b) and how this information sharing structure helps our government combat terror and illicit financing operations. Do you have any suggested legislative improvements to these sections?

Response: Effective information sharing between the government and financial industry, as well as among financial institutions, is critical to combating money laundering and protecting the U.S. financial system. Section 314(a) of the USA PATRIOT Act requires the Secretary of the Treasury to adopt regulations to encourage regulatory and law enforcement authorities to share with financial institutions information regarding persons suspected of engaging in terrorism or money laundering. Pursuant to this authority, FinCEN issued regulations that enable federal, state, local and foreign (European Union) law enforcement agencies and other components of Treasury, through FinCEN, to contact over 16,000 financial institutions to locate accounts and transactions of such persons. In a typical 314(a) request, FinCEN, on behalf of a law enforcement agency, provides a list of subjects/entities to all participating financial institutions, which must respond if they have a positive match.

FinCEN also encourages financial institutions to share information with each other related to money laundering, relying on the safe harbor protection of Section 314(b). Section 314(b) provides a safe harbor from liability that would otherwise arise because of the disclosure of certain customer information between financial institutions. While information sharing under the

314(b) Program is voluntary, it can assist financial institutions in enhancing compliance with their AML/CFT requirements.

One issue frequently noted by industry regarding information sharing is the scope of their safe harbor for information sharing under Section 314(b). The statute currently provides a safe harbor from liability for disclosing information under Section 314(b) for activities that may involve terrorist actions or money laundering activities. Activities that are the predicates for money laundering, like fraud, drug trafficking, cybercrimes, and others, are not explicitly included in the safe harbor. FinCEN did issue guidance on the expansive scope of permissible information sharing covered by Section 314(b) safe harbor in 2009. FinCEN looks forward to working with Congress on ways to continually improve our regulations and the AML/CFT framework.

Question 3: Is FinCEN willing to work with Congress to streamline and modernize the flow of BSA data between financial institutions and the Treasury Department? Can you please provide examples of ways in which we can modernize this process?

Response: FinCEN consistently seeks to improve the efficiency and effectiveness with which it collects and distributes data collected under the Bank Secrecy Act and related statutes, supporting an AML/CFT regime that is one of the most effective in the world. FinCEN is committed to working with the private sector and federal partners through the Bank Secrecy Act Advisory Group and other venues to identify topics and areas for enhancement, ensuring that all stakeholder interests are considered before committing to any solutions.

Questions for the Record for FinCEN Acting Director Jamal El-Hindi
House Committee on Financial Services
Hearing before the Subcommittee on Terrorism and Illicit Finance entitled
"Safeguarding the Financial System from Terrorist Financing"
Thursday, April 27, 2017

Questions for the Record from Representative Bill Foster (IL-11)

Question 1: Over the last decade, we have seen terrorist financiers apply increasingly sophisticated techniques to launder and finance terrorist activities around the world. Which is why effective anti-money laundering and counter-terrorist financing laws are critical to combating the terrorist financing system. Yet, in recent years, financial institutions have paid out billions of dollars in fines, penalties, and forfeitures for violations of the Bank Secrecy Act, the Foreign Corrupt Practices Act, and U.S. sanctions programs. The failure of a financial institution to comply with AML/CFT regulations often has far-reaching consequences for our national security interests. To what extent do these fines and penalties play an important role in enhancing the deterrent value of our AML/CFT framework, and in turn promoting our national security and foreign policy interests?

a. **Given the record number of fines against some of these institutions, do you believe that the penalties are commensurate with the nature of the violations?**
b. **If not, do you have any recommendations in how to address this issue?**

Response: FinCEN is the administrator of the BSA. FinCEN does not have authority to administer or enforce the Foreign Corrupt Practices Act; nor does it have the authority to impose economic sanctions.

The maximum statutory civil money penalty for each BSA violation allows for a potential total amount that, if imposed, could often be deemed excessive and disproportionate to the overall conduct. Accordingly, it is FinCEN's practice to consider all facts and circumstances relevant to an enforcement action, and to impose civil penalties and other remedies that are consistent, fair, and commensurate with the conduct. For example, a financial institution's history of repeat or related violations and noncompliance will militate in favor of significant penalties to ensure future compliance. FinCEN also has the authority to impose undertakings, including monitorships and injunctions to compel remedial action, or to prohibit certain activity, to ensure a financial institution fully complies with its AML/CFT obligations. FinCEN also has the authority to conduct AML/CFT examinations of a financial institution to ensure compliance. FinCEN's written assessment of penalties routinely details the facts underlying the violations, and is issued publicly to inform financial institutions and to serve as a deterrent.