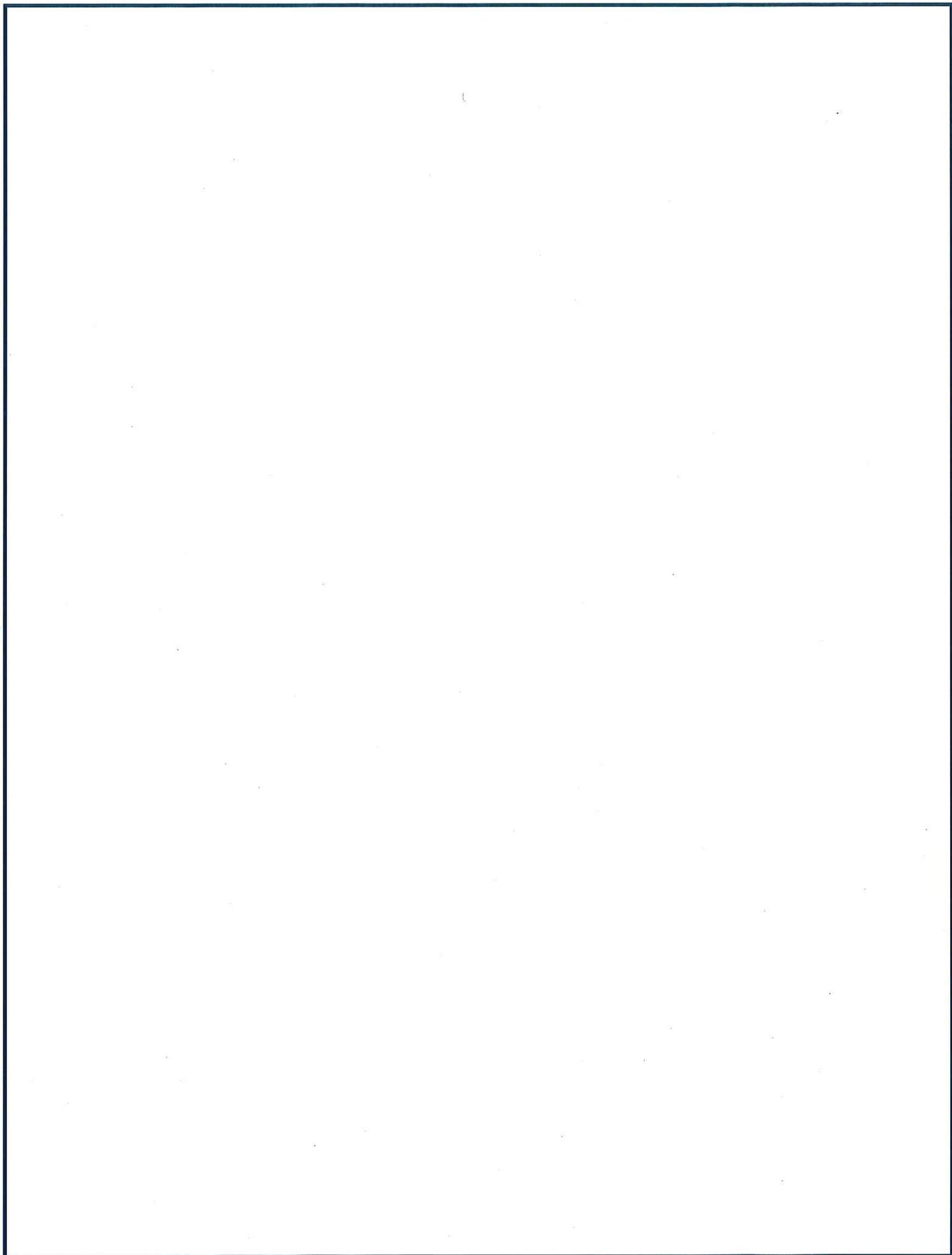




CONGRESSIONAL TASKFORCE ON TERRORISM AND UNCONVENTIONAL WARFARE

4th Parliamentary Intelligence-Security Forum

Vienna, Austria
June 20, 2016





THE HONORABLE ROBERT M. PITTENGER
Chairman

FOR MORE INFORMATION:
(202)225-1976

4TH PARLIAMENTARY INTELLIGENCE SECURITY FORUM

Vienna, Austria
June 20, 2016



(Mr. Werner Amon, Austrian MP; Rep. Robert Pittenger; H.E. Wolfgang Sobotka, Austrian Minister of the Interior; Dr. Andreas Karlsböck, Austrian MP)

Congress of the United States
Washington, DC 20515

Dear Colleague:

Over the past several years, I have hosted three international security forums where there has been consistent participation from approximately 30 countries and up to 100 Members of Parliament. On June 20, 2016, the Congressional Taskforce on Terrorism and Unconventional Warfare co-hosted the 4th Parliamentary Intelligence Security Forum which took place in Vienna, Austria.

This event was co-hosted by several Austrian government officials, including H.E. Wolfgang Sobotka (Austrian Minister of the Interior), Dr. Andreas Karlsböck (Member of Parliament), and Mr. Werner Amon (Member of Parliament). We extend our sincerest thank you for their hard work and dedication that provided an exceptional opportunity for collaboration among international government leaders.

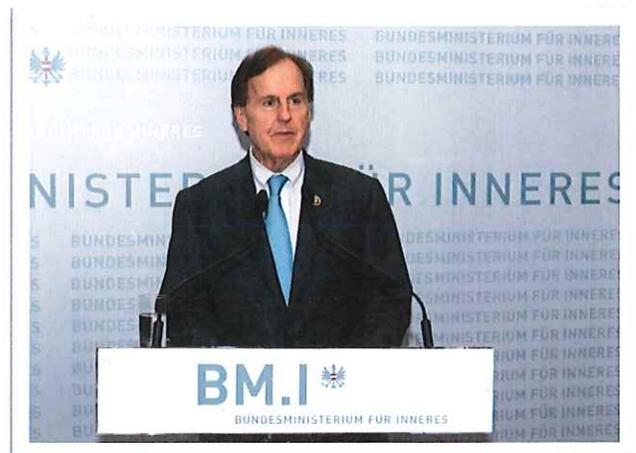
During the event, discussions were held on a variety of international security topics, including terrorist group financing, cybersecurity, and intelligence collaboration. Panelists at this event included a robust American presence, including U.S. active duty military personnel, senior federal government security officials, and private sector experts. Austrian government and judicial experts also participated and provided significant insight throughout the day.

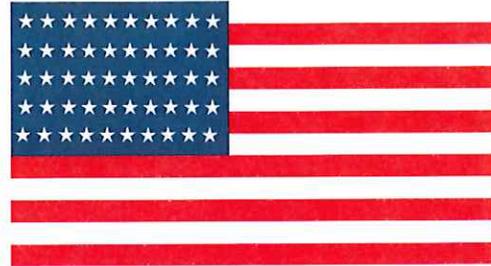
Approximately 30 countries attended our most recent event, and we anticipate follow up events in both the United States and South America. Enclosed you will find an official forum agenda with the list of panelists, a list of foreign participants, an official U.S. State Department summary of events, and published remarks given by the Deputy Director of the Treasury Department's Financial Crimes Enforcement Network.

Thank you for your continued interest in our forum, and we look forward to working with you in the future.



Robert Pittenger
Member of Congress
Chairman, Congressional Taskforce on Terrorism
and Unconventional Warfare





Dear Colleague:

Parliamentary Intelligence Security Forum – an essential conversation tool in a highly endangered world

On June 20, 2016, the 4th *Parliamentary Intelligence Security Forum* took place in Vienna – a city that is not only the capital of modern Austria but was also the heart of an old empire for several centuries. After the terrible World Wars, Vienna has remained a place of international understanding and mediation. Thus, I am glad that the Austrian Federal Ministry of the Interior was ready to host the Security Forum this time.

Two years ago, when I was sitting together with my friend, Congressman Robert Pittenger, in the U.S. Capitol developing the idea of a security conference, I didn't think that it would become such a great story of success. But the high attendance at the 4th meeting at Vienna has confirmed once more the importance and high reputation of this new conversation tool in order to strengthen international parliamentary cooperation on security issues.

At the very beginning – Congressman Pittenger and me – agreed that political decision makers in Europe and in United States should start a dialogue, and in spite of the NSA affair, caused by secret electronic eavesdropping which had irritated people all over Europe and clouded good relationships between our continent and the USA for several months, we held on our project. And it was a right decision. The current global situation confirms dramatically the importance of international cooperation in terms of fighting against terrorism and peace finding.

So it is a great pleasure to me to appreciate the tireless and indispensable efforts of Congressman Pittenger in establishing and organizing the *Parliamentary Intelligence Security Forum*, an invaluable conversation tool that enables assembling Parliamentarians all over the world, particularly the members of the committees responsible for public security an intelligence services. Thanks to Robert Pittenger for this new way of high level discussion in a free atmosphere of trust.

Islamic terrorism continues to threaten the Western world and our way of life. The cowardly attacks towards the editorial office of the French satirical magazine “Charlie Hebdo” showed impressively that we deal with an aggressor who is not to be beat with conventional weapons. More and more people ask for releasing privacy protection in order to succeed in

fighting against this invisible enemy. But more security always correlates with adjusted individual privacy. So we have to find a fair balance between quickest and best possible

providing of confidential information and high level on privacy on the other side – always considering the wise statement of the former US president Benjamin Franklin from 1775: *They who can give up essential liberty to obtain a little temporary safety, deserve neither liberty nor safety.*

Nevertheless we must pay attention that reduction of privacy along the needful fight against terrorism do not weaken our basic democratic values and do not lead in to a total monitoring – George Orwell's greatest nightmare! So we need not only cooperation between governmental organizations and intelligence services responsible for our security – they do a good job, particularly by fighting against spying out and cyber-crime – but also a closer cooperation on high parliamentary level. The 4th *Parliamentary Intelligence Security Forum* in Vienna put a benchmark in finding the right conversation tool aside the daily political agenda, and so it has been really a precious contribution to peace and freedom in our highly endangered world.

Sincerely,

/s/

Dr. Andreas F. Karlsböck
Member of Parliament, Austria

Agenda for the 4th Parliamentary Intelligence Security Forum
on the 20th of June 2016

venue: Austrian Ministry of Interior (co-host),
Minoritenplatz 9 1010 Vienna

Time schedule:

Check-In: 8:30am

Opening: 9:00am

- Welcome speeches:
 - Werner Amon (MP Austria)
 - Andreas Karlsböck (MP Austria)
 - Robert Pittenger (MC USA)
- Opening Remarks on Security Cooperation
 - **Lieutenant General Ben Hodges**, U.S. Army Europe
- Panel I
 - **Jamal El-Hindi**, Dep. Director, Treasury Dept. Financial Crimes Enforcement Network – Terror finance
 - **Mariano Federici**, President, Argentinian Financial Intelligence Unit – Terror Finance
 - **Expert from the FMA (Austrian Financial Market Authority)** (prelim.)
- following discussion
- Panel II
 - **Nikos Passas**, International Anti-Corruption Academy – Terror Finance
 - **Frederick Reynolds**, Managing Director, Global Financial Crimes Compliance Executive, Bank of America – Terror Finance
 - **J.R. Helmig**, Chief Analytics Officer, SAS Corporation – Terror Finance
 - **Mats Nilsson**, Director of Technology, Ericsson – Network Security
 - **Peter Gridling**, Director of the Federal Office for the Protection of the Constitution and Counter Terrorism (prelim.)
- following discussion

Lunch: 12:00pm

Hosted by the Austrian Minister of the Interior H.E. Wolfgang Sobotka

2. Part: 1:30pm

- Panel III
 - **Rachel Brand**, Board Member, U.S. Privacy and Civil Liberties Oversight Board
 - **David Medine**, Chairman, U.S. Privacy and Civil Liberties Oversight Board
 - **Expert from the Constitutional Court of Austria** (prelim.)
- following discussion

- Panel IV
 - **Jason Cassidy**, Dept. of Homeland Security, Homeland Security Investigations, Austrian attaché – Trade-Based Money Laundering
 - **General Franz Lang**, director of the Federal Office of Criminal Investigation (prelim.)
- following discussion

Closing: 5:00pm

Reception: 6pm – 8pm

Hosted by the Embassy of the United States in Vienna, Austria

Location: Residence of Deputy Chief of Mission, Eugene Young
Linnéplatz 4, 1190 Vienna



Attendance list – 4th Parliamentary Intelligence Security Forum

Albania – Arta Dade, MP

Albania – Ben Blushi, MP

Albania – Mimoza Hafizi, MP

Andorra – Tanjit Sandhu Kaur, FIU

Argentina – Juan Félix Marteau

Argentina – Mariano Federici, FIU

Austria - Christoph Karlsböck

Austria - Mag. Thomas Füreder (Speaker FMA)

Austria - Dr. Manfred Andexinger (office Karlsböck)

Austria – Carina Gartner (office Amon)

Austria – Dr. Andreas Karlsböck, MP

Austria – Johanna Resch (office Amon)

Austria – Mag. Bernhard Neumann (Speaker)

Austria – Mag. Gerda Hofbauer (office Karlsböck)

Austria – Mag. Jürgen Kovacic (office Amon)

Austria – Michael Horak (office NEOS)

Austria – Romana Rautner, MA (office Amon)

Austria – Werner Amon, MBA, MP

Bosnia – Borislav Bojić, MP

Bosnia – Ljiljana Milićević, MP

Bosnia – Sifet Podžić, MP

Bosnia – Željko Grubešić, MP

Bulgaria – Atanas Atanassov, MP

Bulgaria – Dimitar Lazarov, MP

Bulgaria – Filip Popov, MP

Bulgaria – Karad Sali Karadayi, MP

Bulgaria – Rada Lessidrenska

Bulgaria – Rumyana Stoyanova – Hristova

Bulgaria – Tsvetan Tsvetanov, MP

Bulgaria – Valentin Kasabov, MP

Cyprus – Marios Ieronymides, Ambassador

Embassy Saudi Arabia Austria – Mr. Anas Alnowaiser

Estonia – Ken-Marti Vaher, MP

European Parliament – Natalia Grecova, MEP

Germany – Andreas Jahn, Assistant of MP Selle

Germany – Christian Flisek, MP
Hungary – Beatrix Kese
Hungary – István Hollik, MP
Hungary – Márta Demeter, MP
Hungary – Márton Balázs
Ireland – Lisa Dardis, MP
Korean Embassy Austria – Agnes Kuderer
Korean Embassy Austria – Botschaftsrat Hanjin-Bae
Latvia – Ainars Latkovskis, MP
Latvia – Osleja Laura (assistant Āboltiņa)
Latvia – Solvita Āboltiņa, MP
Luxembourg – Alex Bodry, MP
Luxembourg – Eugène Berger, MP
Luxembourg – Philippe Donckel, MP
Macedonia – Illir Islami, Embassy
Malta – Angelo Farrugia, MP
Malta – Christopher Said, MP
Malta – Etienne Grech, MP
Norway – Anders Werp, MP
Norway – Kenneth Svendsen, MP
Norway – Ulf Leirstein, MP
Perú – Luis Iberico Núñez, MP
Portugal – Raúl Maia Oliveira (Adviser Pinto)
Portugal – Sérgio Sousa Pinto, MP
Romania – Ambassador Cristian Istrate
Romania – Florin Mitrea, MP
Slovenia – Branko Grims, MP
Sweden – Anti Avsan, MP
Sweden – Arhe Hamednaca, MP
Sweden – Mats Nilsson, Director of Technology, Ericsson
Taiwan Embassy Austria - Archie Yang
Taiwan Embassy Austria - Yu-shun Chen (1st Secretary)
Turkey – Mr. Aydin Ünal, MP
United Kingdom – Ashlee Godwin
United Kingdom – Baroness Buscombe, MP
US Embassy Austria – Andreas Lerch
USA - Clark Fonda

USA - Robert Pittenger, MP

USA - COL David Knych, Senior Defense Official and Defense Attaché

USA - CPT Patrick R. Muldoon, Aide de Camp to Commanding General

USA - LTC Cristine Gibney, Commander's Initiatives Group

USA - LTG Frederick B. Hodges, Commanding General of US Army in Europe

USA - Mr. John Petersen, Deputy Political Advisor

USA - Mr. Lucas Rozsa, USAREUR G2 Analyst

USA – David Medine, Chairman, U.S. Privacy and Civil Liberties Oversight Board

USA – Frederick Reynolds, Managing Director, Global Financial Crimes Compliance Executive

USA – J.R. Helmig, Chief Analytics Officer, SAS Corporation

USA – Jamal El-Hindi, Dep. Director

USA – Jason Cassidy, Dept. of Homeland Security, Homeland Security Investigations, Austrian attaché

USA – Nikos Passas, International Anti- Corruption Academy

USA – Rachel L. Brand, Board Member, U.S. Privacy and Civil Liberties Oversight Board



Dr. Andreas Karlsböck,
Austrian MP



United States Department of State
Official Summary of Parliamentary Forum

Subject: Fourth Parliamentary Intelligence Security Forum in Vienna Calls for Increased Cooperation to Combat Money Laundering and Terrorist Financing:

1. (SBU) *Summary*: Congressman Robert Pittenger joined Austrian counterparts in organizing the Fourth Parliamentary Intelligence Security Forum in Vienna on June 20. The forum served to bring together legislators and officials from 28 European and South American countries to discuss with experts in anti-money laundering (AML) and counter-terrorist financing (CTF) ways to improve cooperation, and to balance privacy and security needs. In his keynote speech, U.S. Army Europe commander Lieutenant General Ben Hodges called on the intelligence community to work toward effectively intercepting the oil trade by ISIL, while panelists urged lawmakers to draft legislation which would balance privacy rights against the need for effective AML/CFT tools. Austrian Interior Minister Wolfgang Sobotka hosted a luncheon for forum participants, delivering a brief welcoming address. *End Summary*



2. (SBU) The Parliamentary Intelligence Security Forum was originally initiated by U.S. Congressman Robert Pittenger (R-NC) and Austrian Parliament Member Andreas Karlsböck from the Austrian Freedom Party (FPÖ) in 2014 as a transatlantic confidence-building

U.S. Privacy and Civil Liberties
Oversight Board

platform in the wake of the NSA disclosures. The meetings, held alternately in Washington and Vienna, Austria, have addressed different aspects of security and intelligence, and the proper legislative role in support and oversight of these activities.

3. (SBU) The panelists in the June 20 meeting were senior U.S. and international experts in combating terrorist financing and money laundering, who addressed 64 legislators and officials from 28 European and South American countries, along with the European Parliament. The presentations and subsequent discussions addressed the need for better cooperation, both locally and internationally. Starting off the day, Rep. Pittenger and MP Karlsböck recalled how the two of them had decided to launch the initiative as a means to conduct transatlantic consultations on sensitive issues such as terrorism, in order to rebuild trust between the U.S. and Austrian and European legislators following the NSA affair. Austrian People's Party (ÖVP) MP Werner Amon formally thanked Pittenger and Karlsböck for the initiative, and the Interior Ministry for co-hosting the event. Amon underscored the importance of transatlantic cooperation and consultations with regard to intelligence sharing and counterterrorism in view of recent terrorist events such as Brussels, Paris, San Bernardino and Orlando

4. (SBU) Jamal El-Hindi, Deputy Director of the U.S. Treasury Department, emphasized the importance of proactive data sharing in order to identify and track foreign terrorist fighters (FTF). El-Hindi critically observed that Financial Intelligence Units (FIUs) were not sharing adequate information with local law enforcement authorities. This was echoed by Rachel Brand, Board Member of the Civil Liberties and Oversight Board, who portrayed the September 11 attacks as a failure of information sharing, underlining the need for free exchange of information in order to prevent similar attacks in the future.

5. (SBU) In his keynote speech, USAREUR Commander Lt. General Hodges described the cooperation among intelligence agencies and local law enforcement authorities as the key to the successful combat against terrorism. In this context, Hodges complained that military units engaged in counterterrorism were frequently prohibited from accessing data on finger prints and retinal scans, which would make it harder for FTFs to travel across borders. He was equally critical



Lt. Gen. Ben Hodges, Commanding General, U.S. Army Europe

of some current legal frameworks, arguing that “soldiers are getting killed because policies do not match reality.” On the specific question of ISIS, General Hodges said it was past time “to find out who was buying the oil from ISIS” – a major source of revenue for the terrorist organization. In reply, a Turkish legislator defended Ankara’s efforts against terrorists and solicited Western solidarity, including a plea for the USG and Europe to place the Syrian Kurdish group YPG on the list of terrorist organizations. Regarding the latter assertion, Lt. General Hodges observed that “the YPG had been the only group in Syria so far effectively battling ISIS.”

6. (SBU) Hodges bemoaned the fact that U.S. law enforcement agencies in Europe were chronically understaffed and rotated in a manner that made it difficult to build sustained professional and confidential relationships with local counterparts. This sentiment was echoed by Frederick Reynolds, Bank of America’s Chief Financial Security Officer, who highlighted the shortage of personnel resources for government authorities, as he noted that Bank of America employed over 800 AML/CTF analysts, while FinCEN had no more than 300 such experts.



Mr. Frederick Reynolds, Bank of America Executive

7. (SBU) Panelists listed various cases where domestic legal restrictions prevented FIUs from sharing information among each other and across borders. Bernhard Neumann, Head of Austria’s Counter Espionage and Non-Proliferation Unit, cited numerous examples where his unit’s investigations were inhibited by Austria’s comprehensive data protection regime, arguing that these laws effectively provided an umbrella that criminals can hide underneath.

8. (SBU) Upon receiving the message that cooperation and current legislation offer considerable room for improvement, the attending legislators were eager to find out what role they could play in the fight against money laundering and terrorism. J.R. Helmig, Chief Analytics Officer of SAS Corporation, recommended that legislators become more involved with FIUs, as the current legislative procedure frequently lacked expert input. Frederick Reynolds, of Bank of America underscored this by outlining the benefits of having an ongoing

dialogue between parliament and institutions, especially with respect to identifying priorities and adapting to different situations.

9. (SBU) In addition to outlining the problems faced by international intelligence agencies when combating terrorism and money laundering, various panelists raised concerns about money laundering activities through trade – an underappreciated challenge.

Mariano Federici, President of Argentina's Financial Intelligence Unit (FIU), explained that transnational criminal organizations frequently use over/under invoicing, over/under shipments, or double invoicing to

mix their illicit funds into the vast export market, where it becomes difficult to trace. These practices become apparent when examining the data in more depth, as export balance sheets often do not match the recipient countries' import balance sheets and authorities often lack the expertise or the will to examine these transactions more closely. Part of the problem stems from distorted incentives, as private sector companies are currently focused on avoiding sanctions, instead of identifying the individuals behind such transactions.



Mr. Mariano Federici, President, Argentina FIU

10. (SBU) Comment: Legislators, the majority from across Europe, broadly praised the Vienna event as a high-caliber, substance-oriented, forum of experts and lawmakers addressing core issues related to international terrorism. Participants appeared eager to learn more about the obstacles the intelligence communities are facing and how they could work towards eliminating these obstacles. There was general agreement with the ongoing need to balance better information sharing with data privacy requirements. Participants also acknowledged the inherent, culture-based distrust that still exists between governments or respective intelligence agencies, particularly when it comes to cross-border information sharing. As with previous meetings, this forum clearly contributed to better understanding among legislators and officials. At an evening reception hosted by Chargé Young, ÖVP MP Werner Amon praised the American contribution to European security, decried the exaggerated criticism too often heard about the U.S. security role, and called for a continuation of the forum, whether in the United States, Europe or, perhaps, Argentina, as FIU chief Federici openly suggested at the conclusion of the forum.



**JAMAL EL-HINDI
DEPUTY DIRECTOR
FINANCIAL CRIMES ENFORCEMENT NETWORK**

**REMARKS AT THE PARLIAMENTARY INTELLIGENCE SECURITY FORUM
JUNE 20, 2016
VIENNA, AUSTRIA**

Good morning. I would like to thank Congressman Pittenger for his invitation to be a part of today's gathering of Parliamentarians for Intelligence Security and for the leadership of this group with respect to this critical issue. It is an honor for FinCEN to be here at the Austrian Ministry of Interior to join in the discussion. Recent events in the United States and elsewhere are difficult reminders that we must remain ever-vigilant in the fight against terrorism, in all of its forms.

The Financial Crimes Enforcement Network, or FinCEN, is a component of the U.S. Department of the Treasury. We are the financial intelligence unit, or FIU, of the United States. We are responsible for collecting, protecting, connecting, and appropriately disseminating financial intelligence to ensure its appropriate use by law enforcement and other stakeholders. We also work with the financial industry to help it safeguard itself from illicit users.

We see time and time again how bad actors such as terrorist financiers, weapons proliferators, drug traffickers, human smugglers, organized crime syndicates, professional money launderers, cybercriminals, tax evaders, rogue regimes, and corrupt officials use the same types of mechanisms to evade detection by the authorities and abuse the financial system. Key to our efforts to understand these threats is working together and sharing information — and it is overcoming potential barriers to information sharing that I will focus on today. We believe that no single jurisdiction can be successful on its own, particularly with respect to terrorism, and the

fact that so many Parliamentarians have gathered here today to discuss these pressing issues tells me that you agree.

As we continue to adapt to ever-evolving threats, we must have the proper legal and regulatory foundation, both in substance as well as process, to ensure that our law enforcement, regulatory, and intelligence professionals, as well as the private sector and our international partners, have the tools that they need in fighting money laundering and terrorist financing. These tools essentially involve the ability to collect financial intelligence information, the ability to analyze it, and the ability to share it responsibly with others.

But collection and use of the information are not the only things that are important to us. Data protection and respect for data privacy are also at stake. In the United States, FinCEN is essentially the embodiment of our government's desire to foster the collection of valuable information from the financial sector for law enforcement purposes, while at the same time protecting the information. In our role, we work to strike a balance between the transparency that allows us to detect and combat threats while at the same time respecting the need for protecting confidentiality and personal privacy. While FinCEN's financial intelligence work thrives on data, we are also responsible for taking a balanced approach to collecting it—making sure that we obtain the right data, while carefully balancing the costs to industry, and being mindful of the need to protect the data that we obtain from misuse. The rules by which we collect this information are subject to public comment, a rigorous process by which we seek to achieve the right balance.

At FinCEN, we receive approximately 55,000 new financial institution filings each day. The majority of the financial intelligence FinCEN collects comes from two reporting streams: one on large cash transactions exceeding \$10,000, and the other on suspicious transactions identified by financial institutions. FinCEN then makes this information available to more than 9,000 law enforcement and regulator users who have been authorized to access the data. Usage of the data is subject to auditing to ensure that appropriate data security and safeguarding protocols are followed. To exploit the data collection, FinCEN also uses "business rules" or algorithms to search the reporting daily for key terms, entities, or typologies of interest. The

rules help us identify reports that merit further review by analysts. Currently, we are running 22 business rules related to ISIL against our data. The results of these rules are provided to our partners in order to bring critical information to their attention much more quickly. FinCEN also develops other products for our partners, such as targeting studies, strategic assessments, and case support.

Using the data to identify connections between and among potential illicit actors is where information sharing becomes especially important. FinCEN disseminates its financial intelligence through secure channels to authorized stakeholders on the widest possible basis both domestically and internationally. The breadth of dissemination is particularly critical in the anti-terrorism context, where we disseminate our information to our law enforcement partners, intelligence authorities, and border police.

Importantly, we also share information with relevant foreign FIUs and pre-authorize those FIUs to further share it with their domestic law enforcement and intelligence agencies. We do this in recognition of the fact that terrorists and terrorist facilitators move from one jurisdiction to another. FinCEN, as the FIU for the United States, recognizes that no one jurisdiction holds all the information necessary to create the full picture of a network of illicit actors, whether they are facilitating terrorism or other crimes. A jurisdiction receiving information from FinCEN, or from another FIU, may have its own information to add to the picture, either right away or over time. The importance of the information may not surface for years. Because we don't know which agency within a jurisdiction might hold the next piece of information that will connect two dots, we promote broad information sharing between the FIUs, their law enforcement, their intelligence agencies, and their border police.

The feedback we are receiving in response to our proactive sharing suggests we are taking the right approach. We have received over 350 positive feedback responses from 41 FIU partners that the financial intelligence we provided to them over just the last eight months either corroborated information related to an ongoing investigation or provided new investigative leads.

Proactive sharing can be particularly useful in the context of dealing with Foreign Terrorist Fighters, or FTFs. Broad sharing of information is essential to mapping out the financial transactions of a known terrorist facilitator and can lead to the identification of previously unknown FTFs. In 2015, U.S. Customs and Border Protection (CBP) reviewed a series of FinCEN analytical reports that included information on a possible terrorism financing network that centered on an individual based in the Middle East. Further research by CBP confirmed that this individual was on the U.S. terrorism watch list, and had received money from dozens of individuals located primarily in Europe, but that he also maintained financial links with individuals in other countries outside Europe. Information provided by our partner FIUs helped draw a larger picture of this network for law enforcement. This example shows how each jurisdiction has a role to play.

FinCEN is not alone in working to stimulate the collection, analysis, and dissemination of financial reporting on FTFs and ISIL financing. Over the last year, FIUs from 40 countries came together as part of a multilateral effort to share information and produce an operational analysis of FTFs, their networks, and common financial indicators. In undertaking this project, which was co-led by FinCEN and the FIU of the Netherlands, we saw a number of obstacles faced by FIUs in doing this type of operational work, many of which related to information sharing.

Since we have a group of lawmakers present, I would like to spend a few minutes discussing some of these obstacles. Here, I want to underscore that, in some respects, the action of Parliamentarians will be needed to improve our global efforts to fight terrorist financing.

First, as a result of our work, we understand that many FIUs are not sharing enough information with or receiving data from their own law enforcement or other domestic agencies. For example, domestic intelligence agencies and customs authorities can be particularly critical sources of information when analyzing foreign terrorist fighters. Prior to 9/11, in the United States, information about threats was kept in different government agencies, where it essentially remained disconnected. After 9/11, particular action was taken by our Congress and our President to facilitate information flow among the various law enforcement and other agencies involved in fighting terrorism. With respect to ensuring that financial intelligence is effectively

used in other jurisdictions, particularly in the fight against terrorism, similar efforts to break down certain barriers might be needed by parliamentarians in other countries.

Second, many FIUs currently face domestic legal restrictions that prevent FIUs themselves from sharing information with one another as effectively as possible. One of the most important, and perhaps most frustrating constraints faced by many countries trying to identify and track FTFs is the inability to share information with other FIUs once an FTF's case has been referred to local law enforcement agencies or prosecutors. Some FIUs, for example, are unable to share information or even acknowledge that they have information in their holdings purely because an investigation or prosecution is ongoing. Such restrictions are not bad in and of themselves. They are meant to protect the integrity of ongoing investigations. This situation is somewhat similar to the impact of the data privacy protection laws that many of us have in place. I say that because, in both situations, the restrictions are meant to serve a compelling public purpose: protecting investigations and/or protecting data privacy. Nevertheless, we must acknowledge that barriers such as these can inadvertently shut down essential information sharing across borders, particularly in the fight against terrorism, where we need to share information as rapidly as possible, given the dire consequences of terrorist acts.

My first two examples involved barriers to information flow between and among government entities. My third example involves a concern that I have heard from the private sector about its ability to share information with FIUs across borders. Our global financial institutions are often positioned to see related activities occurring across borders. However, if the global financial institutions are restricted in sharing information with FIUs across borders, or if FIUs within a jurisdiction are reluctant to receive information that does not pertain primarily to their own jurisdiction, we are squandering an opportunity for the FIU to gain valuable insight from the global financial institution. How is it that an FIU might tell a global financial institution that it does not want to receive information that may only be tangentially related to the jurisdiction? It could be that the FIU is held to a standard of investigating every suspicious transaction reported, regardless of the nature of the STR. If its performance metrics were that rigid, you could see how it might not want to receive what it might at first consider less relevant information. Again, we see how a conceptually reasonable rule — a requirement to investigate

every suspicious transaction report — might lead to the inadvertent consequence of impeding our overall effectiveness.

Identifying and striving to eliminate roadblocks to information sharing such as these in the three examples I have given will help enable FIUs to be more effective partners, within their own countries and with other governments, and will help FIUs take a more proactive approach to the use of financial intelligence. We feel that that this is the right thing to do. But it is not necessarily an easy thing to do.

In each of the three examples, there were good reasons for the barriers, and those good reasons remain. There are reasons why some jurisdictions may want to segregate intelligence agency and law enforcement agency activity; there are reasons why we need to protect investigations; there are reasons for data privacy; and there are reasons why we may hold FIUs to certain metrics to make sure that the information they collect is well used. The challenge to parliamentarians, notwithstanding these good reasons, is to look at the laws and practices in their jurisdictions and make any necessary changes to help promote the collection and appropriate sharing of financial intelligence. Even in the sensitive case of promoting the collection of financial intelligence while also protecting data privacy, don't shy away from the challenge. These two public goods should not be viewed as inconsistent with one another. Indeed, for the sake of protecting the individual liberties which we all hold dear, they must be viewed hand-in-hand as complements to one another.

I would like to end by asking us each to consider one final thing. It is clear that the financial institutions within each of our jurisdictions have responsibilities to aid the fight against money laundering and terrorist financing by monitoring transactions and reporting suspicious activity. And each of our governments have expectations that our financial institutions commit sufficient resources and have strong systems in place to comply with these requirements. But we in government must hold ourselves accountable to similar standards. I feel fortunate to be part of an FIU in a jurisdiction where support for what FinCEN does is evident in all three branches of our government: the executive, the legislative, and the judicial. But, again, the United States is just one jurisdiction. For us to all be successful in our mission, FIUs globally must be well-

resourced in order to fully harness the valuable data they receive from financial institutions. Not all FIUs are in the same situation, and FinCEN does not believe that the way it operates is the only way for an FIU to function. There are different models for different FIUs. But, if an FIU is unable to take advantage of the information that it receives because it is understaffed, underfunded, does not have access to analytical tools, does not have an ability to protect the information, or lacks effective direction, then the efforts of our financial institutions to provide valuable information are lessened and our global efforts against money laundering and terrorist financing suffer. No matter which jurisdiction, each FIU can make a difference. Each FIU, if properly supported, can contribute what may be a critical piece of information in uncovering components of a terrorist network. Each one of us matters in this fight. Please continue your support for our collective mission.

###