AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

THE MUMBAI ATTACKS: A WAKE-UP CALL FOR AMERICA'S PRIVATE SECTOR

HEARING

BEFORE THE

SUBCOMMITTEE ON TRANSPORTATION SECURITY AND INFRASTRUCTURE PROTECTION

OF THE

COMMITTEE ON HOMELAND SECURITY HOUSE OF REPRESENTATIVES

ONE HUNDRED ELEVENTH CONGRESS

FIRST SESSION

MARCH 11, 2009

Serial No. 111–6

Printed for the use of the Committee on Homeland Security

Available via the World Wide Web: http://www.gpoaccess.gov/congress/index.html

U.S. GOVERNMENT PRINTING OFFICE

49–944 PDF WASHINGTON : 2010

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2250 Mail: Stop SSOP, Washington, DC 20402–0001

COMMITTEE ON HOMELAND SECURITY

BENNIE G. THOMPSON, Mississippi, *Chairman*

LORETTA SANCHEZ, California
JANE HARMAN, California
PETER A. DEFAZIO, Oregon
ELEANOR HOLMES NORTON, District of Columbia
ZOE LOFGREN, California
SHEILA JACKSON LEE, Texas
HENRY CUELLAR, Texas
CHRISTOPHER P. CARNEY, Pennsylvania
YVETTE D. CLARKE, New York
LAURA RICHARDSON, California
ANN KIRKPATRICK, Arizona
BEN RAY LUJÁN, New Mexico
BILL PASCRELL, JR., New Jersey
EMANUEL CLEAVER, Missouri
AL GREEN, Texas
JAMES A. HIMES, Connecticut
MARY JO KILROY, Ohio
ERIC J.J. MASSA, New York
DINA TITUS, Nevada
VACANCY

PETER T. KING, New York
LAMAR SMITH, Texas
MARK E. SOUDER, Indiana
DANIEL E. LUNGREN, California
MIKE ROGERS, Alabama
MICHAEL T. MCCAUL, Texas
CHARLES W. DENT, Pennsylvania
GUS M. BILIRAKIS, Florida
PAUL C. BROUN, Georgia
CANDICE S. MILLER, Michigan
PETE OLSON, Texas
ANH "JOSEPH" CAO, Louisiana
STEVE AUSTRIA, Ohio

I. LANIER AVANT, *Staff Director*
ROSALINE COHEN, *Chief Counsel*
MICHAEL TWINCHEK, *Chief Clerk*
ROBERT O'CONNOR, *Minority Staff Director*

SUBCOMMITTEE ON TRANSPORTATION SECURITY AND INFRASTRUCTURE PROTECTION

SHEILA JACKSON LEE, Texas, *Chairwoman*

PETER A. DEFAZIO, Oregon
ELEANOR HOLMES NORTON, District of Columbia
ANN KIRKPATRICK, Arizona
BEN RAY LUJÁN, New Mexico
EMANUEL CLEAVER, Missouri
JAMES A. HIMES, Connecticut
ERIC J.J. MASSA, New York
DINA TITUS, Nevada
BENNIE G. THOMPSON, Mississippi *(Ex Officio)*

CHARLES W. DENT, Pennsylvania
DANIEL E. LUNGREN, California
PETE OLSON, Texas
CANDICE S. MILLER, Michigan
STEVE AUSTRIA, Ohio
PETER T. KING, NEW YORK *(Ex Officio)*

MICHAEL BELAND, *Staff Director*
NATALIE NIXON, *Deputy Chief Clerk*
JOSEPH VEALENCIS, *Minority Subcommittee Lead*

CONTENTS

Page

STATEMENTS

The Honorable Sheila Jackson Lee, a Representative in Congress From the State of Texas, and Chairwoman, Subcommittee on Transportation Security and Infrastructure Protection 1
The Honorable Charles W. Dent, a Representative in Congress From the State of Pennsylvania, and Ranking Member, Subcommittee on Transportation Security and Infrastructure Protection 4
The Honorable Bennie G. Thompson, a Representative in Congress From the State of Mississippi, and Chairman, Committee on Homeland Security .. 5

WITNESSES

PANEL I

Mr. James L. Snyder, Deputy Assistant Secretary, Infrastructure Protection, Department of Homeland Security:
Oral Statement 8
Prepared Statement 10
Mr. Raymond W. Kelly, Commissioner, New York Police Department:
Oral Statement 13
Prepared Statement 17
Mr. James W. McJunkin, Deputy Assistant Director, Counterterrorism Division, Federal Bureau of Investigation:
Oral Statement 20
Prepared Statement 21

PANEL II

Ms. C. Christine Fair, Senior Political Scientist for South Asian Political and Military Affairs, Rand Corporation:
Oral Statement 38
Prepared Statement 41
Mr. David Bradley Bonnell, Director, Global Security, Intercontinental Hotels Group:
Oral Statement 50
Prepared Statement 53
Mr. William G. Raisch, Executive Director, New York University's International Center for Enterprise Preparedness:
Oral Statement 55
Prepared Statement 57

THE MUMBAI ATTACKS: A WAKE-UP CALL FOR AMERICA'S PRIVATE SECTOR

Wednesday, March 11, 2009

U.S. HOUSE OF REPRESENTATIVES,
COMMITTEE ON HOMELAND SECURITY,
SUBCOMMITTEE ON TRANSPORTATION SECURITY AND
INFRASTRUCTURE PROTECTION,
Washington, DC.

The subcommittee met, pursuant to call, at 2:10 p.m., in Room 311, Cannon House Office Building, Hon. Sheila Jackson Lee [Chairwoman of the subcommittee] presiding.

Present: Representatives Jackson Lee, Kirkpatrick, Cleaver, Himes, Titus, Thompson (ex officio), Lungren, Dent, Miller, and King (ex officio).

Ms. JACKSON LEE. The subcommittee will come to order.

The subcommittee is meeting today to receive testimony on "The Mumbai Attacks: A Wake-Up Call For America's Private Sector." Our witnesses today will testify about the November attacks in Mumbai, the groups involved, and what we are doing here to secure American facilities of the type attacked in Mumbai.

I am proud to convene today's hearing to engage our Members and the witnesses on important issues that have arisen from the terrorist attack in Mumbai last November. I sincerely hope that we can learn from the tragic event and apply its lessons to what we are doing to secure the same types of assets in the United States that were targeted in India. In the last 6 weeks, I have been both in Pakistan and in India, and stayed in the Taj in Mumbai, and so I have first-hand, or had a first-hand look on the issues involving this hearing, but more importantly, the question of protecting our infrastructure, because some might ask the question, why a hearing on Mumbai?

This is not necessarily a hearing only on Mumbai. It is asking the serious question of, how do we protect the Nation's infrastructure, and to also ask the next question, how vulnerable is the 85 percent of the Nation's infrastructure held in our private hands? Responsibilities of this Nation, responsibilities of this committee are in fact to protect the homeland.

I do want to welcome our Chairman of the full committee, Mr. Thompson, and thank him for his leadership, and of course, the Ranking Member of the full committee and thank him as well, Mr. King, for his leadership.

As the subcommittee with jurisdiction over the security of critical infrastructure, 85 percent of which is owned by the private sector, it is imperative that we study these types of attacks, our govern-

ment's outreach to its private-sector partners, and whether the private sector is acting on any information provided.

That was a very important question in Mumbai: What kind of information was forwarded to those private owners, and what actions did they take? How did they coordinate with the government? This requires us to have an understanding of the groups involved in the attack and their international aspirations.

I believe today's hearing will shed a great deal of light on these matters, and I am looking forward to our witnesses' testimony and our discussion. We look forward to collaborating in our work with our other subcommittees. The work we do in this committee dealing with critical infrastructure relates to the crisis on the Mexican border that asks the question, will the spill-over violence come on to our shores? Well, our question today, will attacks on infrastructure like hotels, hospitals and schools, in other parts of the world, will they spill on to the soil of the United States? We cannot be unprepared for the probability.

But first, I would like to welcome back the subcommittee's returning Members and welcome the subcommittee's new Members.

In particular, let me welcome our new Ranking Member, Mr. Dent. We thank him very much for his leadership, and I look forward to working with him.

We take note of acknowledging Mr. Cleaver, who is here as a new Member, and we appreciate, again, his participation.

The subcommittee deals in important, interesting, and demanding areas, and I am looking forward to working with all of you in a bipartisan manner to secure the transportation systems and infrastructure that support the American people and their way of life.

I would like to extend an especially warm welcome to the new Ranking Member of the subcommittee, as I indicated earlier, Mr. Dent of Pennsylvania. We look forward to ensuring that this committee answers the concerns of Americans.

The scope of this hearing includes several dynamics, all of which are necessary for us to understand in order to have a better idea about policy going forward. First, DHS, NYPD, and FBI are here to provide an overview of what happened in Mumbai, and we are grateful for their presence here. Both in terms of events and tactics, they will also provide their perspective about what steps need to be taken domestically to secure these types of assets from such attacks.

Second, our witnesses, especially Dr. Fair, from RAND, will be able to shed some light on the group implicated in the attacks, the Lashkar-e-Taiba, or LeT, as well as its potential aspirations beyond South Asia.

Third, we will examine the Department's outreach to the private sector during and in the aftermath of the attack to discern whether it provided private sector stakeholders, such as hotels, with meaningful information about these groups and relevant mitigation measures for bolstering security at their critical assets.

Fourth, we will explore, with the help of Mr. Bonnell from InterContinental Hotels and Mr. Raisch of NYU, the implementation of security efforts at these types of critical infrastructure since September 11, 2001, and the status of security in America's hotels.

As many of you know full well, this committee has the security of our Nation taken very seriously. In the last Congress, we held several hearings on the effectiveness of the Department's approach, and whether voluntary security efforts were working. I am proud of our work in the last Congress, particularly the work in and the legislation involving the 9/11 Act, which sought to promote private-sector security in a market-based manner, and I stand ready to make improvements where they are necessary.

In the 111th Congress, we will build our strong record and continue to engage in thoughtful and robust oversight of these issues. But passing legislation is key as well. We look forward to doing so, just as we are very proud of the language we put in the 9/11 bill that created the Transportation Security Centers of Excellence.

There is more to be done legislatively to help our local law enforcement and to protect the critical infrastructure of America. In this context, the attack in Mumbai offers us a pivotal moment to reassess whether we are securing the types of targets that are being attacked world-wide, hotels, hospitals, rail stations, and I have mentioned schools, universities. Whatever we need to do to improve that, we must do it.

We must also understand emerging tactics of groups like LeT, and whether our local law enforcement community is prepared to subdue them quickly and effectively. It must be said that DHS has taken many important steps to make America more secure since it was created, and the multidimensional issue of critical infrastructure protection cannot be resolved overnight. This subcommittee stands ready to aid the efforts of all stakeholders, whether Federal, State, local, or in the private sector, but we ask them to ask us for help as we reach out to help them.

The time line of the events in Mumbai are familiar to many of us. On the evening on November 26, 2008, 10 men arrived in Mumbai, India, by way of small boats in the Arabian Sea and attacked a number of high-profile targets with automatic weapons and explosives. The physical site made it more evident as I viewed it. The water is very close to the Taj and there were no barriers, nothing to protect the people inside the hotel. By the time the siege was over, they had killed more than 160 people in many places around the city and terrorized the city for more than 60 hours.

Among the sites attacked in Mumbai, India's business and entertainment capital, were two luxury hotels, the Taj and the Oberoi, along with the main railroad terminal, a Jewish cultural center, a cafe frequented by foreigners, a cinema house, and two hospitals. In fact, it was the Chabad House. Six Americans were among the 26 foreigners killed. These sites were and are the very types that we are concerned about, and we are committed to work with State and local law enforcement entities as well as the private sector. DHS is charged to protect those. As we continue to work on this issue, we will continue to be assured that we will look to new weapons and technology to see how we can prevent these kinds of attacks.

It has become clear that attacks carried out in this kind of style, suicide incidents that saw nine of those involved killed, are something that we need to be concerned about. A recent op-ed in the New York Times by a professor at the Naval Postgraduate School

posited that "right now, most of our cities would be as hard-pressed as Mumbai was to deal with several simultaneous attacks."

My friends, the question is: How vulnerable are we? The question is: As we answer that one, how will we be prepared?

Am I concerned? Absolutely. That is why this hearing is being held today.

It is my pleasure now to recognize the gentleman from Pennsylvania, Mr. Dent, for an opening statement.

Mr. DENT. First, thank you, Madam Chairwoman.

Let me start off by saying how pleased I was that Ranking Member King appointed me as the Ranking Member of the Subcommittee on Transportation Security and Infrastructure Protection.

I thank you very much for that, Mr. King.

This subcommittee has a very ambitious oversight legislative agenda this Congress, and I very much look forward to working with the gentlelady from Texas in securing our Nation from terrorist threats to its aviation and critical infrastructure components. I thank you for your gracious welcome here, and I look forward to working with you over the course of this session.

Let me also, of course, welcome the Ranking Member of the full committee, the gentleman to my immediate left from New York, Mr. King, who has made it his mission to ensure that the Federal Government takes a risk-based approach in managing Homeland Security approach. Also I would say similarly to that the Chairman of the full committee, Mr. Thompson of Mississippi, I know also very much embraces a risk-based approach to dealing with our Nation's homeland security issues.

So welcome to both of you.

Let me also recognize our new Members of the subcommittee, some of whom will be arriving here over the course of the hearing, deputy Ranking Member and also a fellow Texan, that is Mr. Olson; the gentlelady from Michigan, Ms. Miller; and the gentleman from Ohio, Mr. Austria.

Today's hearing will explore the Mumbai terror attacks that occurred last Thanksgiving. However, rather than rehash what the Senate examined 3 months ago, I want to focus on the way forward on what the Department is doing to prepare for a similar attack in the United States and how it is working with State and local law enforcement as well as private-sector representatives.

It took 12 hours for the Indian Emergency Services personnel to arrive on scene, and 10 terrorists, using everyday communication systems, held a nation hostage for more than 2 days while they methodically killed hundreds of innocent bystanders. A 12-hour response time is simply unfathomable. I wanted to know with certainty that such a broken response scenario could never happen here in the United States.

I truly appreciate the competing demands for all of your time, and so I thank all the witnesses for coming before the subcommittee today, and I look forward to your testimony. At this time, I yield back the balance of my time.

Thank you, Madam Chairwoman.

Ms. JACKSON LEE. I thank the distinguished gentleman from Pennsylvania. It is my pleasure to yield now to the Chairman of

the full committee, the gentleman from Mississippi, Mr. Thompson, who as I indicated, has been forthright on so many issues impacting the Nation's security.

The gentleman from Mississippi is recognized.

Mr. THOMPSON. Thank you very much, Madam Chairwoman, and I welcome our first panel of witnesses to this hearing.

For more than 60 hours last November, the world watched as Mumbai, India's entertainment and financial capital, was terrorized by attacks on hotels, hospitals, the main railway station, and other public places. By the time the siege was over, 11 terrorists had killed more than 160 people using automatic weapons and explosives. The style of attack, the weapons, the technology used, and the diversity of the targets raise new questions for how we should approach counterterrorism and security measures here at home at all levels of government and in the private sector.

It has become clear that the type of attack carried out in Mumbai, a Fedayeen-style attack, where small groups engage in combat operations, as distinguished from suicide bombings, pose a challenge to our soft targets in our law enforcement community.

The committee has jurisdiction over the security of critical infrastructure, 85 percent of which is owned by the private sector. As such, it is critical that we study this emerging Mumbai-style of attack, evaluate how well DHS engages private-sector partners in efforts to secure against such attacks, and review how the private sector acts on shared information.

By examining DHS's outreach to the private sector, during and in the aftermath of these attacks, we can determine whether it provided stakeholders, such as hotels, with actionable information about the threat situation, the groups involved and the mitigation measures to be implemented.

DHS, NYPD and the FBI will address what happened in Mumbai, both in terms of events and tactics, as well as how information was shared in the United States. They can also provide insight into domestic measures we can implement to secure these types of assets from similar attacks.

Dr. Fair, from RAND, will provide us with perspectives on the group implicated in the attacks, LeT, as well as its potential for operating outside of the South Asia region.

Witnesses from InterContinental Hotels and NYU will address the implementation of security efforts at these types of critical infrastructures since September 11, 2001, and the status of security in America's hotels.

I look forward to the testimony of all the witnesses today at this hearing about efforts to secure America's critical infrastructure throughout the Congress.

I yield back.

Ms. JACKSON LEE. Thank you very much, Mr. Chairman, for your remarks. Much appreciated.

The Chair now recognizes the Ranking Member of the full committee, the gentleman from New York, Mr. King, for an opening statement, with the acknowledgment that one of his constituents has been gracious enough to be part of this hearing.

I yield the gentleman the customary 5 minutes.

Mr. KING. I thank you, Chairwoman Jackson Lee.

I want to thank you for your courtesy today and also for the great job you do as Chair, and also Mr. Dent, who I know will do an outstanding job as your Ranking Member, and of course, my good friend Bennie Thompson, Chairman Thompson, who, he and I had a very wonderful lunch with Commissioner Kelly in New York a few years ago. Even then, I was perceptive enough to know that Bennie might be the Chairman some day, so I wanted to get him on the good side of New York. Sure enough, he became the Chairman, and he has been a staunch ally for the whole concept of risk-based funding.

I want to welcome all the witnesses today.

General, I certainly wish you the very best on your job.

Deputy Assistant Director, we certainly appreciate your efforts.

Commissioner Kelly, of course, I have known for many years and know first-hand the terrific job that he does with the NYPD.

It happened in Mumbai, and it reminded us, all of us, how easy it could happen here. So I certainly look forward to the testimony today, especially Commissioner Kelly's, because he has brought the private sector so much into what has to be done in New York.

General Snyder, that is part of your responsibility, also, on a national level.

I think it is particularly important that we have hearings like this, because for instance, just last week in New York, the New York Times said that we should not be talking about terrorism, that we shouldn't be scaring people. Well, I think Mumbai showed just how essential it is that we do keep a level of awareness, a heightened state of awareness, because, to me, too many people have forgotten what happened on September 11; the fact that 7½ years has gone by without an attack, we can put it in the recesses of our mind, just like it was 8½ years between the first World Trade Center attack and the second. So I think, despite maybe certain elements in the media who say we shouldn't talk about it, if we don't talk about it, if you don't go out and do your job and keep the public engaged, they are not going to realize how vital this is.

So I really commend all of you for keeping your sense of direction and your sense of motivation so high, and especially Commissioner Kelly of New York, and General Snyder. You have to keep the public engaged in this. You have to keep the private sector engaged. I give you credit for doing it, because, unfortunately, too many people have forgotten how terrible it was and how real a threat it can be.

I also want to emphasize again the importance of cooperation between all of the levels of government. Ranking Member Dent and Chairwoman Jackson Lee spoke about the long delay that happened in Mumbai. We could not tolerate that here in the United States. I know that, certainly just speaking from the New York perspective, knowing how closely engaged the NYPD is with the Coast Guard and with Homeland Security, with the FBI, with the State police, how essential that is. I look forward in your testimony during the questioning to see again whether all of you feel that the level of cooperation is sufficient.

Also, when we are talking about risk-based funding, what more has to be done on that as far as getting the type of training, the type of equipment, the type of technology into, especially in large

cities like New York, Chicago, Boston, Las Vegas, Houston, where you could have this type of attack, where a hotel could be taken over, a house of worship could be taken over, a subway system could be taken over, how, what more has to be done in that regard?

Also, General, I would really be interested in, and you have only had a few weeks on the job, but what do you think the level of public sector interest is in this? Are they willing to cooperate? I wonder, if the city has not been attacked, do they realize how important it is that they do work with the police?

Also, obviously Homeland Security, but Homeland Security is always going to be somewhat removed. I believe for it to be successful, you have to have the private sector working with the local Police Department and State officials, and what you think the level of interest is around the country, or do we see too much of what we saw in the New York Times where people just say, ignore terrorism, and somehow it will go away or whatever the thinking is?

So, anyway, I look forward to all your testimony. This is a vital, vital issue, and I think the Chairwoman, I know the Chairwoman deserves tremendous credit for taking an international issue and showing why it is such, unfortunately, such a local, State, and national issue to the United States of America and such a really vital Homeland Security issue.

So, Chairwoman, again, I thank you for calling this hearing. I thank the witnesses for being here. I thank the Chairman and the Ranking Member.

I yield back.

Ms. JACKSON LEE. Mr. Ranking Member, thank you for your remarks. It just causes me, again, to repeat the name of this committee, in terms of its focus on transportation, security, and infrastructure protection, very important elements, but also the name of the hearing, "The Mumbai Attacks: A Wake-up Call for America's Private Sector." I might edit it and say private and public sector, and that is what we hope the testimony will present us with this afternoon.

It is my pleasure to acknowledge Mr. Himes, who is a Member of the committee and brings great leadership and also knowledge. We thank you for you presence here.

I want to also acknowledge, I believe, Mr. Austria here and thank him for his presence. We know, with Members' schedules that they will be here in the hearing room. We thank them all for their presence.

I welcome our first panel of witnesses. Our first witness is Major General Jim Snyder, the Deputy Assistant Secretary for Infrastructure Protection at the Department of Homeland Security. In his capacity, he helps to lead the coordinated national effort to reduce the risk to the Nation's critical infrastructure posed by acts of terrorism and in increasing the Nation's preparedness, timely response, and rapid recovery in the event of an attack, natural disaster, or other emergency. In particular, he works with the private sector to secure our Nation's critical infrastructure.

Our second witness, Commissioner Ray Kelly, of the New York Police Department, whom I had the pleasure of meeting with earlier on this very issue, and I thank him for his courtesies, was appointed police commissioner of the city of New York by Mayor Mi-

chael Bloomberg in 2002, making Commissioner Kelly the first person to hold the post for the second time in his career.

Prior to his current position, Commissioner Kelly was a commissioner of the U.S. Customs Service, where he managed the agency's 20,000 employees and $20 billion in annual revenue. Commissioner Kelly spent 31 years in the New York City Police Department, serving in 25 different commands and as police commissioner from 1992 to 1994.

It was reported last month that the NYPD launched a counterterrorism initiative to train a new team of officers in tactics for close quarters combat and rescuing hostages in hotels and other high-rise buildings. This initiative was an immediate response to lessons NYPD learned from Mumbai.

Our third witness, James W. McJunkin, is the Deputy Assistant Director of the FBI Counterterrorism Division. Mr. McJunkin has been with the FBI for nearly 22 years. In 2005, Mr. McJunkin was selected as the Assistant Special Agent in Charge of the Washington, DC, Field Office, where he provided leadership and supervision to the Joint Terrorism Task Force, provided management to all substantive counterterrorism investigations conducted within the National Capital Region and supervised a number of significant overseas investigations involving terrorism attacks against U.S. citizens.

In March 2006, he has led a team of FBI investigators with the on-scene investigation of a terrorist attack against the U.S. Consulate in Karachi, Pakistan, that claimed the life of a career diplomat and several foreign nationals. On January 24, 2008, Director Mueller designated Mr. McJunkin as the Deputy Assistant Director for FBI Counterterrorism Operations, branch one.

We appreciate very much the experience you bring to us this afternoon.

Without objection, the witnesses' full statements will be inserted in the record. I now ask each witness to summarize his statement for 5 minutes.

Before I conclude on that, acknowledging Deputy Assistant Secretary Snyder, let me also indicate that Members will have the opportunity to submit their statements into the record. We do appreciate it, without objection.

Beginning now with the testimony from the witnesses, we will begin with the Deputy Assistant Secretary Snyder.

STATEMENT OF JAMES L. SNYDER, DEPUTY ASSISTANT SECRETARY, INFRASTRUCTURE PROTECTION, DEPARTMENT OF HOMELAND SECURITY

Mr. SNYDER. Thank you, Chairwoman Jackson Lee and Ranking Member Dent and Members of the subcommittee.

I appreciate the opportunity to discuss the DHS Office of Infrastructure Protection interaction with our Government and private-sector partners during the Mumbai, India, attacks.

The Mumbai attack reminds us that terrorism remains very real and that those who wish us harm are remaining dangerous and can adapt quickly. The commando-style attacks were well-planned, well-coordinated and well-executed, striking multiple targets in the transportation and commercial facility sectors. The attacks were

aided by the targets' open access, which presents an inherent security challenge.

We also must adapt to this dynamic threat environment and to similar dangers posed by catastrophic natural events by remaining flexible and strengthening our coordination efforts with the Government and private sector.

IP activities are based on the framework outlined in the National Infrastructure Protection Plan which was released in 2006 and updated in 2009. Our mission is to work closely with our Government and private-sector partners across the 18 critical infrastructure and key resource sectors to lead the effort to secure and enhance the resiliency of the Nation's infrastructure.

Because most critical infrastructure is owned and operated by the private sector, the Department leverages partnerships to achieve success. We have successfully established more than 40 voluntary partnership councils among Government and private-sector entities. The value of these relationships has been well demonstrated in local and national responses to hurricanes, fire, and other incidents.

During Mumbai, IP worked directly with the commercial facilities, banking and finance, and transportation sectors and religious organizations to share information and organize a response. On November 26, we disseminated reports on common vulnerabilities, potential indicators of terrorist activity and protective measures to our sector partners through the Homeland Security Information Network for Critical Sectors—it goes to a 4,500-member user community—so that they could implement and increase their security posture.

On the 27th, IP released the TRIPwire Significant Incident Report on the attacks to over 6,000 users in the TRIPwire community. TRIPwire is the Department's collaborative networks for bomb squads, law enforcement, and other emergency services personnel. IP issued three additional TRIPwire postings over the next 13 days and updated HSIN–CS on December 1.

On December 2, IP's commercial facilities Sector-Specific Agency coordinated a conference call with over 200 leaders across the 18 sectors. On December 9, IP hosted a table-top exercise based on a multiple IED attack with representatives from all 18 sectors, and we reinforced the Mumbai lessons learned.

On December 10, a conference call was held for 75 leaders of the banking and financial sector. On January 12, INA and IP conducted a classified briefing for senior security directors of major hotel chains and other commercial ventures, providing a detailed analysis of the Mumbai attacks.

On January 29, IP's commercial facilities Sector-Specific Agency led a terrorism simulation exercise. It was conducted with the Real Estate Roundtable subsector, and designed around a Mumbai-style attack. Prior to the exercise, IP presented the roundtable a briefing and discussion on the Title IX Voluntary Private Sector Preparedness Program, now called PS–Prep, as we have to all sectors, and we think that this program will become a positive step forward in the process. These are only a few examples of activities with our partners that build the relationships and processes we use during response to an all-hazard event.

Critical IP work is conducted in the field by Protective Security Advisors. ADPSAs are in place around the Nation to assist with State, local, and private-sector efforts to protect critical assets. During national disasters and contingency events, PSAs work in State and local emergencies to provide real-time information on protective measures.

It is important to note that individual facility owners and operators and their State and local officials know a specific asset and are best positioned to lead coordination of security and emergency response planning. DHS's role is to facilitate, provide expertise and tools to augment that planning, and advise on protective measures and response actions.

I believe the next attack may be prevented when law enforcement or the private sector see something specific and take immediate action. We have seen that many times before. This, coupled with communications strengthened during hurricane experiences, has developed operational linkages that enable effective planning in advance of an incident, increase security and resiliency of our Nation's infrastructure, and produce the operational effect of a quick response should an incident occur.

Thank you for your attention. I would be happy to answer any questions you may have at this time.

[The statement of Mr. Snyder follows:]

PREPARED STATEMENT OF JAMES L. SNYDER

MARCH 11, 2009

Thank you, Chairwoman Jackson Lee, Ranking Member Dent, and Members of the subcommittee. I appreciate the opportunity to participate in the hearing "The Mumbai Attacks: A Wake-Up Call for America's Private Sector," and to discuss the Department of Homeland Security's Office of Infrastructure Protection's interaction with our Government and private sector partners during and following the terrorist attacks in Mumbai, India.

As acknowledged with this hearing, the Mumbai attack on November 26–30, 2008, served as a strong reminder that the threat of terrorism remains very real, and that those who wish us harm remain dangerous and adapt quickly to changing circumstance. The terrorist attacks were well-planned, well-coordinated, and well-executed. The terrorists carried out a complex attack and struck multiple targets in the transportation and commercial facilities sectors, particularly hotels and religious locations. One example of their ability to adapt was their decision to shift tactics and conduct a water-borne entry rather than the normal overland entry to the target area, thus avoiding observance. Their attacks were also facilitated by the targets' business requirements for open access, a reality that represents an inherent security challenge. This type of attack highlights the vulnerabilities of soft targets, and how difficult it is to prepare, prevent, and respond to such attacks.

Consequently, we too must adapt to this dynamic threat environment—as well as to the dangers posed by catastrophic natural events—by remaining both nimble and flexible in our approach to infrastructure protection, and by continuing to enhance our coordination efforts with government at all levels and with the private sector.

IP activities are based on the framework and approach outlined in the National Infrastructure Protection Plan (NIPP). Our mission is to work closely with our Government and private sector partners across the 18 critical infrastructure and key resources (CIKR) sectors and to lead the effort to ensure that a comprehensive, multi-faceted framework exists to secure and enhance the resiliency of the Nation's CIKR. Because the majority of the Nation's CIKR are owned and operated by the private sector, the Department must leverage partnerships and relationships to achieve success. Using the NIPP framework, the Department has successfully established primarily voluntary partnerships among interested Federal, State, local, tribal, and private sector entities. These partners work within the framework to set goals and priorities, identify key assets, assign roles and responsibilities, allocate resources, and measure progress against national priorities. DHS released the NIPP

in 2006 and, following its first triennial review and update, recently re-released it as the 2009 NIPP. The subtitle of the 2009 NIPP is "Partnering to Enhance Protection and Resiliency."

The value of the relationships we have built through this partnership has been demonstrated in local and national response to hurricanes, fires, and other real world incidents. In the steady-state environment, we sustain these relationships through information sharing, exercise, and training so that when an incident occurs, whether man-made or natural, we can respond and recover effectively and efficiently. For example, on December 9, 2008, IP hosted a tabletop exercise based on a multiple improvised explosive device attack with representation from all 18 critical infrastructure sectors. Additionally, IP's Commercial Facilities Sector Specific Agency Executive Management Office (SSA–EMO) participated in a January 29, 2009, Terrorism Simulation Exercise. The tabletop exercise, Threat & Response Options—Public Communications Challenges, was conducted with the Commercial Facilities Real Estate Roundtable subsector. The exercise was designed around a Mumbai-style attack and facilitated active discussion on preventive, response, and recovery activities. These are only two of many exercises we conduct annually with our CIKR partners that build the relationships and processes we use during response to all-hazards events.

In the case of Mumbai, IP worked directly with the Commercial Facilities Sector, Banking and Finance Sector, Transportation Sector, and leadership from religious organizations to share relevant information. To facilitate information collection, analysis, and distribution, IP leveraged the incident management capabilities built into its Incident Management Cell (IMC). The IMC is a cross-functional operations group that provides the core staff and facilities around which IP's scalable incident management capability coalesces during a large-scale CIKR incident. Prior to the Mumbai incident, the IMC provided effective leadership and coordination in communicating with our partners during Hurricanes Gustav and Ike. IP's response is guided by the National Response Framework and National Incident Management System which enable a systematic approach to response operations.

IP's initial actions on the first day of the Mumbai attacks, November 26, were to disseminate Common Vulnerabilities (CV), Potential Indicators of Terrorist Activity (PI), and Protective Measures (PM) Reports to public and private sector partners through the Homeland Security Information Network for Critical Sectors (HSIN–CS) portal and its 4,500-member user community. These reports provide security officials with specific information on potential vulnerabilities and recommendations on specific protective measures that they can implement to increase their security posture.

On November 27, IP released a TRIPwire Significant Incident Report (SIR) to provide information on the attacks to over 6,000 users in the TRIPwire community. TRIPwire is the Department's on-line, collaborative, information-sharing network for bomb squads, law enforcement, and other emergency services personnel. It provides continuously updated information about current terrorist improvised explosive device (IED) tactics, techniques, and procedures, including design and emplacement techniques. IP issued three additional TRIPwire postings over the next 13 days. These updates provided detailed analysis of the terrorist tactics, techniques, and procedures, and recommended protective measures based on the employed strategies. These updates, along with a Mumbai TRITON Special Report, were also shared with members of the private sector through postings on the HSIN–CS portal. TRITON reports are monthly or incident-reactive reports that assess terrorist tactics, techniques, operations, and strategies. TRITON reports are produced by a UK-based subject matter expert company, and are provided by IP to our State and local government TRIPwire users.

On December 1, IP e-mailed an updated TRIPwire SIR that contained additional information to all TRIPwire system users and the National Infrastructure Coordinating Center (NICC). IP also posted the SIR to the TRIPwire web site "What's New" Portal and to HSIN–CS. Of note, during the 8-day time frame of November 27 to December 4, TRIPwire had over three times the average number of site visits, indicating intense user interest in the Mumbai attacks and the terrorist tactics, techniques, and procedures used in the attacks.

On December 2, IP's Commercial Facilities SSA–EMO coordinated a conference call with over 200 leaders across all sectors. The Department's Office of Intelligence and Analysis (I&A), Homeland Infrastructure Threat and Risk Analysis Center (HITRAC), IP, and Transportation Security Administration provided detailed information on the Mumbai attacks to call participants. Their briefings included analyses of the tactics, techniques, and procedures used in the Mumbai attack, and provided security recommendations to address these attack methods. Specific protective measures were proposed to address surveillance, target selection, infiltration, target

access, and engagement with security forces. Based on positive feedback from that call, an additional conference call was held on December 10 specifically for 75 leaders of the Banking and Finance Sector.

On January 12, I&A and IP conducted a classified briefing for senior security directors representing major hotel chains and other commercial venues. The briefing provided a detailed analysis of the tactics, techniques and procedures used in the Mumbai attacks, including specific details of the IEDs; terrorist exploitation of technology; surveillance techniques; timeline of the attack including the targets and tactics; and recommended protective measures for surveillance, port security, access control, and coordination with security forces on specific actions to improve the security posture at their location.

In addition to the interactions with our NIPP partners in Washington, DC, a significant portion of IP's work is conducted in the field, across the United States, by the Protective Security Advisor (PSA) cadre. Eighty PSAs are in place in communities throughout the Nation to assist with State, local, and private sector efforts to protect critical assets, providing a Federal resource to communities and businesses. During natural disasters and contingency events such as Mumbai, PSAs often work in State and local Emergency Operations Centers. PSAs also provide real-time information on facility significance and protective measures to facility owners and operators, as well as State and local representatives. For example, during the Mumbai event, the PSA for Las Vegas met with hotel, casino, and resort security officials to answer questions and distribute our CV/PI/PM reports that provide details on enhanced security recommendations and best practices.

PSAs also conduct Enhanced Critical Infrastructure Protection (ECIP) assessment visits to assess overall site security, identify gaps, recommend protective measures, educate facility owners and operators on security, and promote communication and information sharing among facility owners and operators, DHS, and State governments. Information collected during ECIP visits will be used to develop ECIP metrics; conduct sector-by-sector and cross-sector vulnerability comparisons; identify security gaps and trends across CIKR sectors and sub-sectors; establish sector baseline security survey scores; and track progress toward improving CIKR security through activities, programs, outreach, and training. This information is utilized during incidents to help focus national and local response efforts on identified areas of criticality within the impact area and assist in the prioritization of reconstitution efforts.

In addition to the PSA program, IP has provided support for reducing risk of a terrorist attack to the Nation's CIKR by conducting vulnerability assessments for assets in the Commercial Facilities Sector. The Buffer Zone Protection Program (BZPP) is a DHS-administered grant program designed to help local law enforcement and owners and operators of CIKR increase security in the "buffer zone"—the area outside a facility that can be used by an adversary to conduct surveillance or launch an attack. The BZPP focuses on identifying and mitigating vulnerabilities at the highest-risk critical infrastructure sites and is designed to increase local law enforcement capabilities and preparedness.

Additional support is provided through Site Assistance Visits (SAVs). These are "inside the fence" vulnerability assessments conducted jointly by IP in coordination and cooperation with Federal, State, local, and CIKR owners and operators that identify critical components, specific vulnerabilities, and security enhancements. During an SAV, consequence and vulnerability information is collected to inform risk data, which is then used as supporting information for risk-based decision-making.

IP has also conducted training for more than 1,900 stakeholders in the Commercial Facilities Sector and law enforcement officials who protect assets in the Lodging and Resorts Subsectors. Relevant courses include Soft Target Awareness, Surveillance Detection, IED Awareness, and Protective Measures.

To provide additional assistance to the Commercial Facilities Sector, IP is currently deploying Risk—Self-Assessment Tool (R–SAT), an upgraded, re-engineered version of the Vulnerability Identification Self-Assessment Tool (ViSAT). ViSAT is a Web-based self-assessment tool developed by IP and provided free of charge to CIKR asset owners/operators, primarily in places of mass gatherings such as arenas and stadiums. This tool assists owners/operators to raise the level of security at CIKR facilities and establish a common baseline of security from which all assets in certain sectors or subsectors can identify weaknesses and establish protection plans. Modules have currently been deployed for stadiums, arenas, convention centers, performing arts centers, and speedways. Commercial facilities members currently have access to ViSAT, and DHS has provided a grant to the International Association of Assembly Managers, a co-chair of the Public Assembly Subcouncil, to promote and provide training for this tool.

IP also provides the Constellation/Automated Critical Asset Management System (C/ACAMS) to State and local communities at no cost. Currently, 30 States use C/ACAMS, a CIKR asset management system that focuses on the unique requirements and information needs of first responders. It provides vulnerability and consequence scoring tools that aid the user's subjective analysis of criticality; an integrated open source information portal, Constellation, which ties together critical asset data and reporting about the current threat environment; a tailored reporting capability to assist in data calls on critical assets; Buffer Zone Generation capability; capability to generate pre-incident operational plans; on-line resources for first responders; and an integrated geographic information system via the Department's Integrated Common Analytical Viewer.

Additionally, the Regional Consortium Coordinating Council (RCCC) was established in Fall 2008 to bring the unique perspectives of geographically based public and private partnerships into the NIPP framework. The RCCC comprises existing functional and active regional entities that include both Government and private sector members. The RCCC provides a critical link between CIKR owners/operators and key homeland security officials and activities at the regional, State, and local levels.

These Departmental efforts and resources are critically important. However, as we move forward and enhance our efforts, and recall the lessons learned from Mumbai, it is also important to acknowledge that individual facility owners and operators, and their State and local officials, know the unique circumstances facing a specific asset and are, therefore, best positioned to serve as primary lead in coordination of security and emergency response planning. DHS's role is to facilitate and augment planning and support where necessary and appropriate.

I believe a key opportunity to prevent the next attack in this country will be by local law enforcement and the private sector seeing something suspicious and taking action or calling that information into the proper authorities. Time and again, we have witnessed this effective solution both here in the United States during the Fort Dix and South Carolina incidents and overseas. The Federal Government and the Department of Homeland Security can and do assist with these efforts by providing valuable information to our local Government and private sector partners.

As I have described, IP is focused on continuing to improve our capability to provide timely and actionable information to our public and private sector partners. This, coupled with partnerships strengthened during recent hurricane experiences, has reinforced the operational linkages that will enable effective planning in advance of an incident, result in enhanced safety, security and resiliency of our Nation's CIKR, and produce an operational effect for expeditious, efficient, and effective response should an incident occur.

Thank you for your attention, and I would be happy to answer any questions you may have at this time.

Ms. JACKSON LEE. I thank the gentleman for his testimony.

I would like to acknowledge the presence of Congresswoman Titus from Nevada. We appreciate her service on this committee.

I now recognize Commissioner Kelly to summarize his statement for 5 minutes.

STATEMENT OF RAYMOND W. KELLY, COMMISSIONER, NEW YORK POLICE DEPARTMENT

Mr. KELLY. Thank you, Madam Chairman.

Chairman Thompson, Congressman King, Congressman Dent, Members of the subcommittee, thank you for the opportunity to testify about the New York City Police Department's response to the terrorist attacks in Mumbai.

I want to begin my remarks by saying that partnership with the private sector has been a hallmark of the NYPD's counterterrorism program since 2002. It is our collective responsibility to learn from events like those that took place in Mumbai and adapt our programs to prevent them. That is exactly what we have endeavored to do in New York.

We have a program called NYPD Shield that includes over 6,000 private security personnel who train with us and function as addi-

tional eyes and ears. We held a briefing with 400 members of this group immediately after the attacks in Mumbai. At that meeting, we had the lead officer in a three-man team that we sent to Mumbai call in from Mumbai and share the lessons that we learned with the audience.

I will update you on our response to those lessons shortly. Before I do that, I want to make you aware of a more recent study conducted by our intelligence division analyzing the similarities between the Mumbai assault and the attack in Lahore, Pakistan, on March 3, targeting the Sri Lankan national cricket team. Eight people were killed in that incident, including six Pakistani police officers. That terrorists would attack a cricket team to attract maximum attention should not come as a surprise considering the sport's immense popularity in South Asia. Last year when the NYPD formed a cricket league as part of our outreach efforts with the South Asian community in New York City, it received scant attention in the New York media but was widely covered in India, Pakistan, and other countries in South Asia and Europe.

The attacks in Mumbai and Lahore are evidence of a shift in tactics from suicide bombs to a commando-style military assault with small teams of highly trained, heavily armed operatives launching simultaneous sustained attacks. We are paying very close attention to this trend.

Other similarities we identified include choice of location; dense, relatively unprotected urban areas where the terrorists could establish strategic choke points to impede the response of authorities.

We also know that some form of detailed pre-attack surveillance was carried out in both cases, as evidenced by the terrorists' thorough familiarity with their target.

Likewise, both sets of attackers coordinated their movements closely through the use of basic technology, cell phones in Mumbai and small battery-powered two-way radios in Lahore.

The assault teams themselves are composed of physically fit males between the ages of 20 and 30. They were similar in composition and in size with 10 people involved in the Mumbai attack and an estimated 12 in Lahore.

In each instance, the teams appeared to break down into smaller two-man operating units once the attack was launched.

In both Mumbai and Lahore the attackers were armed with assault rifles, semiautomatic pistols, and grenades. They carried backpacks with additional ammunition and explosives, more than enough to sustain a prolonged siege. The attackers were casually attired in Western clothing with oversized jackets, button-down shirts and cargo-style pants that could conceal contraband.

Both groups were calm, unhurried, and methodical. They also carried food and drugs to enhance their performance and stamina. In Mumbai, the terrorists reportedly used cocaine and amphetamines to stay awake. In Lahore, remnants of unspecified high-energy foods were recovered from the scene.

It appears both attacks were not initially designed to be suicidal. The goals of the terrorists include hostage taking, extending the violence and the resulting media coverage, and escaping. In Mumbai, the terrorists were able to take captives. However, they were captured or killed before they issued demands or escaped. In Lahore,

they were unsuccessful in taking hostages, but they did manage to evade capture.

Both operations focused on highly symbolic targets. By impacting tourism and international sports, they were intended to instill fear and cause economic damage. They were also aimed at attacking the global reputations of India and Pakistan and heightening regional tensions between the two.

While the political root causes of these attacks appear to be local, the terrorist networks behind them are global, well-funded, and interconnected. The militant Islamic groups suspected in these cases, mainly Lashkar-e-Taiba, have deep and long-standing ties to al Qaeda. In fact, LeT has trained such terrorists as convicted shoe bomber Richard Reid and Essa Al Hindi, who surveilled buildings in New York's financial district prior to September 11. They are also believed to have trained militant Islamic fighters for conflicts around the world, including in Iraq and Afghanistan. As far as we know, they have not directly targeted a Western country, but they specifically sought out locations in Mumbai with Western and Jewish clientele. Hopefully we won't see their tactics migrate to the United States, but if they do, we certainly intend to be prepared.

Within hours of the end of the attacks in Mumbai, the NYPD began making arrangements to send personnel there. This is in keeping with the practice we followed for several years. In all cases, our officers do not take part in investigative activity. In Mumbai, our officers toured crime scenes, took photographs, and asked questions of police officials.

They relayed what they learned back to New York. These officers are a part of a Police Department overseas liaison program in which we have posted experienced personnel to 11 cities around the world. They partner with local police and intelligence agencies and respond when terrorist incidents occur.

In this case, the most senior officer in the group had served as the liaison in Amman, Jordan. In July 2006, when seven bombs exploded in Mumbai trains and rail stations, he flew to the city on a similar mission. The relationships he forged during that trip proved helpful in December.

Our liaisons arrived in Mumbai on December 2, 3 days after the attacks ended. By December 5, our intelligence division had produced an analysis which we shared with the FBI. As I noted that morning, we convened a special meeting with the members of NYPD Shield. During the live conference call with our team leaders in Mumbai, we posted photographs and maps to help the audience visualize the locations he was describing.

We also conducted two exercises, one a tactical drill for emergency service unit officers, the other a table-top exercise for commanders. Both scenarios mirrored the attacks in Mumbai.

Based on our analysis of what took place in Mumbai, we have been training additional officers to use heavy weapons in close quarter battle tactics. In the event of a sustained attack such as you saw in India, these officers will be able to support and relieve the more than 400 members of our emergency service unit who already have these skills.

Last month, 134 officers from our Organized Crime Control Bureau became the first to complete the new course of heavy weapons

and tactics training. We are continuing this month with another group of 135. Our goal is to qualify up to 1,500 officers in these special skills.

We also provided basic heavy weapons instruction for our most recent class of over 1,000 police recruits. We will do the same for our current academy class.

In Mumbai, the local police were simply outgunned by the terrorists. We don't want that to happen in New York. We are also meeting with service providers to see if a means can be developed to pinpoint disruption of cell or satellite phones used by a terrorists during an attack without the wholesale disruption of communications in the immediate vicinity.

We also saw that, in Mumbai, the local authorities had insufficient knowledge of the layouts of targets. In light of this observation, we have assigned our emergency service unit supervisors to tour major hotels and other landmarks. Out of each visit, they develop a briefing book with a description of the location and detailed diagrams, as well as a video that can be used for training purposes. We have conducted 11 in-depth tours of major hotels so far, and we are continuing to select new locations.

At our December 5 Shield meeting, we also reviewed a list of best practices in hotel security. This is a set of items we routinely share when our counterterrorism officers conduct training with hotel security.

Through another partnership, Operation Nexus, NYPD detectives have made thousands of visits to the kind of companies terrorists might seek to exploit, truck rental businesses, scuba diving schools, or hotels. We let them know what to look for and what to do if they observe suspicious behavior.

As part of this initiative we have assigned a senior officer to work exclusively with hotels. After Mumbai, he and his team visited numerous hotels where they met with security directors and developed emergency procedures to use in the event of a Mumbai-style attack.

As part of our training, we also emphasize with hotel staff the importance of knowing who is inside and recognizing that the attack may be initiated from within the facility. We talk about how to identify hostile surveillance or the stockpiling of materials, controlling points of entry, and having a thorough knowledge of the building's layout and a widely distributed emergency action plan.

We also ask the hotel personnel to be acutely aware of suspicious behavior on the part of visitors, such as denying staff access to rooms for extended periods, loitering on guest floors or in the lobby, requesting specific rooms, receiving unusual parcels, and inquiring about hotel security. Along with an array of other sensitive landmarks, major hotels are also the site of visits by our Hercules teams and critical response vehicles.

In addition to hotels, locations also include hospitals, houses of worship, critical infrastructure and tourist attractions, such as Times Square.

While we have to learn from Mumbai and Lahore and prepare to defend ourselves against similar attacks, we cannot focus too narrowly on any one preventive method.

Ms. JACKSON LEE. Commissioner, are you wrapping up?

Mr. KELLY. I am. I am sorry. I apologize.

Ms. JACKSON LEE. We want to hear you. Just wanted to——

Mr. KELLY. Let me stop here.

I want to thank you for inviting me, Madam Chairwoman.

[The statement of Mr. Kelly follows:]

PREPARED STATEMENT OF RAYMOND W. KELLY

MARCH 11, 2009

Chairman Thompson; Chairwoman Jackson Lee; Congressman King; Congressman Dent; Members of the subcommittee.

Thank you for this opportunity to testify about the New York City Police Department's response to the terrorist attacks in Mumbai. I want to begin my remarks by saying that partnership with the private sector has been a hallmark of the NYPD's counterterrorism program since 2002. It is our collective responsibility to learn from events like those that took place in Mumbai, and adapt our programs to prevent them. That is exactly what we've endeavored to do in New York.

We have a program called NYPD Shield that includes over 6,000 private security personnel who train with us and function as additional eyes and ears. We held a briefing with 400 members of this group immediately after the attacks in Mumbai. At that meeting, we had the lead officer in a three-man team we sent to Mumbai call in from overseas and share the lessons we learned with the audience.

I will update you on our response to those lessons shortly. Before I do that, I want to make you aware of a more recent study conducted by our Intelligence Division analyzing the similarities between the Mumbai assault and the attack in Lahore, Pakistan on March 3 targeting the Sri Lankan national cricket team. Eight people were killed in that incident, including six Pakistani police officers.

That terrorists would attack a cricket team to attract maximum attention should not come as a surprise considering the sport's immense popularity in South Asia. Last year, when the NYPD formed a cricket league as part of our outreach efforts with the South Asian community in New York City, it received scant attention in the New York media but was widely covered in India, Pakistan, and other countries in South Asia and Europe.

The attacks in Mumbai and Lahore are evidence of a shift in tactics from suicide bombs to a commando-style military assault with small teams of highly trained, heavily armed operatives launching simultaneous, sustained attacks. We're paying very close attention to this trend.

Other similarities we identified included the choice of locations: dense, relatively unprotected urban areas where the terrorists could establish strategic choke points to impede the response of authorities. We also know that some form of detailed, pre-attack surveillance was carried out in both cases, as evidenced by the terrorists' thorough familiarity with their targets. Likewise, both sets of attackers coordinated their movements closely through the use of basic technology: cell phones in Mumbai and small, battery-powered two-way radios in Lahore.

The assault teams themselves were composed of physically fit males between the ages of 20 and 30. They were similar in composition and in size, with 10 people involved in the Mumbai attack and an estimated 12 in Lahore. In each instance, the teams appeared to break down into smaller, two-man operating units once the attack was launched.

In both Mumbai and Lahore the attackers were armed with assault rifles, semi-automatic pistols and grenades. They carried backpacks with additional ammunition and explosives, more than enough to sustain a prolonged siege. The attackers were casually attired in western clothing, with oversized jackets, button down shirts and cargo style pants that could conceal contraband.

Both groups were calm, unhurried, and methodical. They also carried food and drugs to enhance their performance and stamina. In Mumbai, the terrorists reportedly used cocaine and amphetamines to stay awake. In Lahore, remnants of unspecified high energy foods were recovered from the scene.

It appears both attacks were not initially designed to be suicidal. The goals of the terrorists included hostage-taking, extending the violence and the resulting media coverage, and escaping. In Mumbai, the terrorists were able to take captives. However, they were captured or killed before they issued demands or escaped. In Lahore, they were unsuccessful in taking hostages but they did manage to evade capture.

Both operations focused on highly symbolic targets. By impacting tourism and international sports they were intended to instill fear and cause economic damage.

They were also aimed at attacking the global reputations of India and Pakistan and heightening regional tensions between the two.

While the political root causes of these attacks appear to be local, the terrorist networks behind them are global, well-funded, and interconnected. The militant Islamic groups suspected in these cases—mainly Lashkar-e-Taiba—have deep and long-standing ties to al Qaeda.

In fact, L.E.T. has trained such terrorists as convicted shoe-bomber, Richard Reid, and Essa Al Hindi who surveilled buildings in New York's financial district prior to September 11. They are also believed to have trained militant Islamic fighters for conflicts around the world, including in Iraq and Afghanistan. As far as we know, they have not directly targeted a western country but they specifically sought out locations in Mumbai with western and Jewish clientele. Hopefully, we won't see their tactics migrate to the United States, but if they do we intend to be prepared.

Within hours of the end of the attacks in Mumbai, the NYPD began making arrangements to send personnel there. This is in keeping with a practice we have followed for several years. In all cases, our officers do not take part in investigative activity. In Mumbai, our officers toured crime scenes, took photographs, and asked questions of police officials. They relayed what they learned back to New York.

These officers are part of the Police Department's overseas liaison program in which we post experienced personnel to 11 cities around the world. They partner with local police and intelligence agencies and respond when terrorist incidents occur. In this case, the most senior officer in the group had served as a liaison in Amman, Jordan. In July 2006, when seven bombs exploded in Mumbai trains and railway stations, he flew to the city on a similar mission. The relationships he forged during that trip proved helpful in December.

Our liaisons arrived in Mumbai on December 2, 3 days after the attacks ended. By December 5, our Intelligence Division had produced an analysis, which we shared with the FBI. As I noted, that morning we convened a special meeting with the members of NYPD Shield. During the live conference call with our team leader in Mumbai, we posted photographs and maps to help the audience visualize the locations he was describing.

We also conducted two exercises, one a tactical drill for Emergency Service Unit officers, the other a tabletop exercise for commanders. Both scenarios mirrored the attacks in Mumbai.

Based on our analysis of what took place in Mumbai, we've been training additional officers in the use of heavy weapons and close quarters battle tactics. In the event of a sustained attack, such as we saw in India, these officers will be able to support and relieve the more than 400 members of our Emergency Service Unit who already have these skills. Last month, 134 officers from our Organized Crime Control Bureau became the first to complete this new course of heavy weapons and tactics training. We're continuing this month with another group of 135. Our goal is to qualify up to 1,500 officers in these special skills. We've also provided basic heavy weapons instruction for our most recent class of over 1,000 police recruits. We will do the same with our current class. In Mumbai, the local police were simply outgunned by the terrorists. We don't want that to happen in New York.

We are also meeting with service providers to see if a means can be developed to pinpoint disruption of cell or satellite phones used by terrorists during an attack, without the wholesale disruption of communications in the immediate vicinity.

We also saw that in Mumbai, the local authorities had insufficient knowledge of the layouts of the targets. In light of this observation, we've assigned our Emergency Service Unit supervisors to tour major hotels and other landmarks. Out of each visit they develop a briefing book with a description of the location and detailed diagrams, as well a video that can be used for training purposes. We've conducted 11 in-depth tours of major hotels so far and we are continuing to select new locations.

At our December 5 Shield meeting we also reviewed a list of best practices in hotel security. This is a set of items we routinely share when our counterterrorism officers conduct trainings with hotel security personnel.

Through another partnership, Operation Nexus, NYPD detectives have made thousands of visits to the kind of companies terrorists might seek to exploit: truck rental businesses, scuba diving schools, or hotels. We let them know what to look for and what to do if they observe suspicious behavior.

As part of this initiative, we've assigned a senior officer to work exclusively with hotels. After Mumbai, he and his team visited numerous hotels where they met with security directors and developed emergency procedures to use in the event of a Mumbai-style attack.

As part of our training, we also emphasize with hotel staff the importance of knowing who's inside and recognizing that the attack may be initiated from within

the facility. We talk about how to identify hostile surveillance or the stockpiling of materials, controlling points of entry and having a thorough knowledge of the building's layout and a widely distributed emergency action plan.

We also ask hotel personnel to be acutely aware of suspicious behavior on the part of visitors, such as: denying staff access to rooms for extended periods; loitering on guest floors or in the lobby; requesting specific rooms; receiving unusual parcels; and inquiring about hotel security.

Along with an array of other sensitive landmarks, major hotels are also the sites of visits by our Hercules teams and Critical Response Vehicle Surges. The former consist of heavily armed members of our Emergency Service Unit, who appear unannounced at key locations in a show of force designed to disrupt terrorist surveillance. This is also the goal of our daily CRV surges, in which large convoys of patrol cars proceed with emergency lights and sirens to a pre-arranged site based on intelligence. In addition to hotels these locations include hospitals, houses of worship, critical infrastructure, and tourist attractions like Times Square.

All of the measures I have discussed are part of a robust counterterrorism program we built from the ground up in 2002, when we realized that it in addition to our focus on crime-fighting, the Police Department needed to build the intelligence collection, analysis, and infrastructure protection capabilities to defend New York City from another terrorist attack.

We established the Nation's first municipal counterterrorism bureau, and we restructured our Intelligence Division. We recruited the best that the Federal Government had to offer to head those two operations. We created a new civilian intelligence program to support our field commanders with timely information and analysis. We tapped the incredible linguistic diversity of the police department. We assigned native speakers of languages such as Arabic, Urdu, and Pashto to counterterrorism duties. We strengthened our patrols of key infrastructure in the city, including bridges, tunnels, and a host of landmarks and other sensitive locations. We forged collaborative relationships with the private sector, with law enforcement organizations up and down the east coast, and with Federal agencies, especially the FBI and the Department of Homeland Security.

In the last 7 years, working with the FBI through the Joint Terrorism Task Force, we've stopped multiple plots against New York City. I know that this productive collaboration will continue to thrive.

The Police Department's strongest and most innovative regional partnership is the one supported by the Department of Homeland Security, our Securing the Cities program. This is an unprecedented initiative to protect New York with advanced radiation detection devices installed at all points of access to the five boroughs, including roads, bridges, tunnels, and waterways. We now train and share information with dozens of neighboring jurisdictions.

Our collaboration with the Federal Government has been essential. Through the Homeland Security, Transit Security, and Port Security Grant Programs, among others, we have instituted effective and innovative programs. In the past, the NYPD worked directly with the Transportation Security Administration to obtain grants and steer Federal funds to the most effective programs. We believe it is vitally important to maintain this direct connection and to ensure that DHS's transit security program preserve its distinct mission, purpose, and management, without undue bureaucratic layers. It is our hope the Congress will work with the new leadership at DHS to ensure that the agencies with the shared mission of protecting the transit system be allowed to work together.

While we have to learn from Mumbai and Lahore and prepare to defend ourselves against similar attacks, we cannot focus too narrowly on any one preventive method. We need to strengthen our defense on every front, stay sharp, well-trained, well-equipped, and constantly vigilant. And we must continue to work together at every level of government and with the private sector to defeat those would harm us.

I want to thank the committee Members for your crucial support in making this possible, and for this opportunity to update you on our initiatives.

Ms. JACKSON LEE. We look forward to the opportunity to engage in questioning. Thank you for that very helpful testimony.

It is my pleasure now to recognize Mr. McJunkin to summarize his statement for 5 minutes. The gentleman is recognized.

STATEMENT OF JAMES W. MCJUNKIN, DEPUTY ASSISTANT DIRECTOR, COUNTERTERRORISM DIVISION, FEDERAL BUREAU OF INVESTIGATION

Mr. MCJUNKIN. Good afternoon, Chairwoman Jackson Lee, Ranking Member Dent and Members of the committee. Thank you for inviting me here today to discuss lessens learned from the recent terror attacks in Mumbai, and how the FBI is working with our U.S. and international intelligence and law enforcement partners to apply those lessons to protect the homeland and U.S. interests overseas.

Within hours of the first attacks on Mumbai, the FBI had a representative on the scene, the assistant legal attaché to our New Delhi office, who was traveling in the direction of Mumbai when he was notified of the attacks. He immediately made his way to the Taj Mahal hotel.

Ms. JACKSON LEE. Mr. McJunkin, is your microphone on, or could you move it closer to you, please? Thank you.

Mr. MCJUNKIN. He immediately made his way to the Taj Mahal hotel, which was still under siege, and contacted his Indian counterparts. From there, he took part in the rescue of Americans trapped in the hotel. He also worked with the U.S. Embassy to obtain approval from the Indian government to deploy our Los Angeles Rapid Deployment Team and key personnel from FBI headquarters to assist with the investigation.

The team, which arrived in Mumbai on November 29, had two major jobs. One is the pursuit of justice, which involves traditional forensic-based investigative work to track down those who were murdered Americans and determine who the attackers co-conspirators were. Two, and equally important, is the prevention mission, which involves generating new information to determine who else might still be out there who potentially poses a threat to the United States, our citizens, and our allies.

The investigation continues, and we still have personnel in India who have been working with our Indian law enforcement and intelligence partners to help uncover information about how the attacks were executed, how the attackers were trained, and how long the attacks took to plan. We have been sharing that information with our Federal, State, and local and international law enforcement partners and using it to bolster our efforts to protect the homeland.

So far, the Mumbai attacks have reinforced several key lessons. One, terrorist organizations don't need weapons of mass destruction or even large quantities of explosives to be effective. The simplest weapons can be as deadly. It comes as no surprise, therefore, that a small disciplined team of highly trained individuals can wreak that level of havoc that we saw in Mumbai. Last week's attack on the Sri Lankan cricket team in Lahore, Pakistan, is another example of a low-tech but potentially high-impact operation. We are concerned about the possibility that other foreign terrorist groups, including al Qaeda or its affiliates, will take note of those attacks and attempt to emulate them.

The take-home lesson for the FBI and DHS is that we must continue to look at both large and small organizations with the right combination of capability and intent to carry out attacks. Two, we need to reenergize our efforts to keep the American public engaged

and vigilant. That is critical to the effort to prevent something like the Mumbai attacks from occurring on our shores. As we engage the public, we want to encourage them to be cognizant of and report suspicious activity that comes to their attention to their local, State, and Federal law enforcement agencies.

A key tool for engaging the public and our law enforcement partners is Guardian, a Web-based application to track suspicious incident reporting. As we receive information on threats from law enforcement, other Federal agencies, and the general public, we input these reports into the system where they can be tracked, searched, analyzed, and triaged for action. No threat report is left unaddressed. Although roughly 97 percent of these incidents are ultimately determined to have no conclusive nexus to terrorism, we believe we cannot afford to ignore potentially important threat indicators.

We have begun a pilot deployment of eGuardian, an unclassified system that enables participation by our State, local, and tribal law enforcement partners. eGuardian will enable near real-time sharing and tracking of terrorist information and suspicious activities among State, local, and tribal and Federal entities.

Another key lesson the Mumbai attacks reinforced is the importance of international partnerships. As Director Mueller said during his visit to India and Pakistan last week, terrorism is not an issue for one country alone. We are all fighting a common enemy. We all continue to work with our counterparts in India and around the world to bring the perpetrators of these attacks to justice and to prevent further attacks.

In conclusion, Madam Chairman, as the threats to the United States become more global, the FBI is expanding our collaboration with our law enforcement and intelligence partners here at home and around the world. We are working with our international counterparts to prevent terrorist attacks and assist in their investigation when they do occur. As we have done with the Mumbai attacks, we will continue to analyze and share lessons learned from these investigations to help prevent future attacks at home or against U.S. interests abroad. Thank you.

[The statement of Mr. McJunkin follows:]

PREPARED STATEMENT OF JAMES W. MCJUNKIN

MARCH 11, 2009

Good afternoon Chairwoman Jackson-Lee, Ranking Member Dent, and Members of the committee. I appreciate the opportunity to be here today to discuss the FBI's role in investigating the November 2008 terrorist attacks in Mumbai, India. I will also describe how we are working with our U.S. intelligence and law enforcement partners to apply lessons learned from the Mumbai attacks to protect the U.S. Homeland, as well as how we are collaborating with our international partners to help prevent attacks on U.S. interests and our allies overseas.

FBI ROLE IN MUMBAI INVESTIGATION

As the committee knows, on November 26, 2008, several men armed with hand grenades, automatic weapons, and satellite phones landed in a rubber raft on the shores of Mumbai. They scattered to soft targets across the city, launched simultaneous attacks that held India's financial capital under siege for days, and killed more than 170 individuals, including six American citizens. Within hours of the first attacks, the FBI had a representative on the scene: our Assistant Legal Attaché in the FBI's New Delhi office, who was traveling in the general direction of Mumbai

when he was notified of the attacks. He immediately made his way to the Taj Mahal hotel, which was still under siege, and contacted his Indian counterparts. From there, he took part in efforts to rescue Americans trapped in the hotel, set up lines of communication with his FBI and U.S. Intelligence Community (USIC) counterparts, and coordinated the arrival of our Los Angeles Rapid Deployment Team.

Even before the crisis ended, the investigation had begun. Agents from FBI offices in New Delhi, Islamabad, and Los Angeles joined forces with the Indian government, the CIA, the State Department, and foreign partners. Through these partnerships, we had unprecedented access to evidence and intelligence. Agents and analysts interviewed more than 70 individuals, including the sole surviving attacker. Our forensic specialists pulled fingerprints from improvised explosive devices. They recovered data from damaged cell phones, in one case by literally wiring a smashed phone back together.

At the same time, we collected, analyzed, and disseminated intelligence to our partners at home and abroad—not only to determine how these attacks were planned, and by whom, but to ensure that if a second wave of attacks was planned, we had the intelligence to stop it.

I also want to acknowledge the very fine work that the FBI's Office of Victim Assistance, working in concert with U.S. consular officers in Mumbai and the State Department's Bureau of Consular Affairs, undertook to assist the U.S. citizen victims and their families. That work continues to this day.

THREATS POSED BY SUSPECTED SPONSORS OF MUMBAI ATTACKERS

The surviving Mumbai attacker has claimed that the Pakistan-based terrorist organization Lashkar-e-Tayyiba (LT) provided him training and direction for the attack. The FBI assesses that LT, which is well known to the U.S. Intelligence Community (USIC), remains a threat to U.S. interests in South Asia and to the U.S. homeland. We have no current intelligence indicating that there is an organized LT presence in the United States or that LT senior leadership is seeking to attack the U.S. homeland. LT does maintain facilitation, procurement, fundraising, and recruitment activities worldwide, including in the United States. For example, in 2003, several followers of "Virginia Jihad" cleric Sheikh Ali Al-Timimi were convicted of providing material support to terrorism relating to their training at an LT-sponsored training camp in Pakistan, with the intention of fighting against Coalition Forces in Afghanistan. In addition, the FBI is investigating a number of individuals across the United States who are linked in some way to LT—primarily through witting and unwitting fundraising for the group, as well as the recruitment of individuals from the United States to attend LT camps.

LESSONS LEARNED FROM MUMBAI ATTACKS

The principal lesson from the Mumbai attacks remains that a small number of trained and determined attackers with relatively unsophisticated weapons can do a great deal of damage. Last week's attack on the Sri Lankan cricket team in Lahore, Pakistan, is another example of a low-tech, but potentially high-impact operation. We are concerned about the possibility that other terrorist groups, including al Qaeda or its affiliates, will take note of these attacks and attempt to emulate them.

The FBI is implementing the lessons learned from the Mumbai attacks by continuing to maintain a high level of vigilance for all indications of developing terrorist activity. We recognize that the planning for the Mumbai attacks likely unfolded over a relatively long period of time with careful surveillance of the target sites and transportation routes. We are continuing to work closely with our State, local, and tribal law enforcement partners in our Joint Terrorism Task Forces to follow up on indications of suspicious activity that could potentially be related to terrorism.

We are also sharing relevant information from the Mumbai investigation with our intelligence and law enforcement partners. Classified information is available to cleared State and local law enforcement personnel in Joint Terrorism Task Forces and Fusion Centers. In addition, the FBI and the Department of Homeland Security (DHS) jointly issued an unclassified alert about the attacks to State, local, and tribal officials on November 27, 2008. The FBI and DHS also issued an Intelligence Bulletin on December 3, 2008, to building owners and operators, as well as the law enforcement community, to alert them to preliminary findings regarding the techniques and tactics terrorists used in the Mumbai attacks. The bulletin indicated that the FBI and DHS had no credible or specific information that terrorists were planning similar operations against public buildings in the United States, but urged local authorities and building owners and operators to be aware of potential attack tactics. We continue to work with our partners to heighten the public's awareness

of the continued threat of terrorist attacks and the need to report suspicious incidents.

One key lesson the Mumbai attacks have reinforced is the importance of international partnerships. The unprecedented collaboration we developed with our Indian law enforcement and intelligence counterparts in this investigation has strengthened our relationship with the Government of India. As Director Mueller said during his visit to India and Pakistan last week, terrorism is not an issue for one country alone—we are all fighting a common enemy. We will continue to work with our counterparts in India, and around the world, to bring the perpetrators of these attacks to justice, and to prevent further attacks.

CONCLUSION

As the investigation into the Mumbai attacks progresses, FBI counterterrorism agents and analysts continue to analyze all available information to determine who was responsible, assess lessons learned, determine if the United States may be vulnerable to a similar attack, and determine the threat posed by the group—or individuals tied to the group—to the United States. We are working closely with our USIC and law enforcement partners in these efforts, and will continue to disseminate information about lessons learned.

In summary, Madam Chairwoman, as the threats to our Nation and our allies become ever-more globalized, the FBI is expanding our collaboration with our international and U.S. law enforcement and intelligence partners to prevent terrorist attacks and to assist in investigating them when they do occur. We will continue to build on these relationships to advance the FBI's national security mission. And, as we have done with the Mumbai attacks, we will continue to analyze and share lessons learned from these investigations to help prevent future attacks at home or against U.S. interests abroad.

Ms. JACKSON LEE. Let me thank the witnesses for their testimony. I am looking forward to the opportunity, again, of all our Members being able to engage.

I will remind each Member that he or she will have 5 minutes to question the panel. I will now recognize myself for questions.

Let me start with you, Mr. Secretary Snyder, and each person I would appreciate answering the question. How vulnerable are we in America? Is it important that we recognize that the vulnerabilities today still exist with respect to an attack on our infrastructure?

Mr. SNYDER. Well, Madam Chairwoman, certainly, we use a process beginning with a risk assessment that goes through every sector to determine the vulnerabilities that are common across sectors as well as within facilities in that sector. We have an annual process called the SHIRA, which seeks input from all the sectors, as well as States for the facilities that they think are at most risk.

We look and develop a national risk profile. This year it is based on an all-hazards risk, which is a wider-based risk approach than what we have had in the 2008 risk assessment, and that was based on a terrorist-specific risk. So we measure risk in a relative sort of way, across the sectors, based on the vulnerabilities of those facilities, based on the capabilities that the terrorists or other disasters could have on that facility, and then the consequences, you know, that would be impacted upon the local populace, either economic or certainly loss of life and property.

Ms. JACKSON LEE. So you do an analysis to determine so?

Mr. SNYDER. Yes, ma'am.

Ms. JACKSON LEE. I think, in addition to the analysis it is important to have real-life experiences as well, and I hope that that is part of your assessment.

Commissioner Kelly, how many hotels in America, and again, this is a question that is rhetorical. But what is your thought about

whether our hotels today in America have preparation plans that would have addressed the commando attacks? Would you also answer the question: How vulnerable do you think we are in large sites, as in a hotel or stadium, around the country?

Mr. KELLY. Well, any free society is going to be vulnerable. There is no question about it that we are vulnerable. The issue is: What can we do to reduce that vulnerability? I can really only speak for New York, what we have done. We have done a lot. We certainly intend to do more.

I think the hotel industry, as the title of this hearing says, I think they have had a few wake-up calls here, certainly in Islamabad and certainly in Mumbai, and I think they are responding to it. But it is difficult to redesign hotels. I mean, these are standing structures.

I can tell you what we do. I mentioned in my lengthy prepared remarks that we do talk to the industry, literally, on a daily basis, the hotels in New York. We work with them as far as developing best practices. We do inspections; we communicate that information to them.

But, you know, there is only so much that you can do. We are going to continually remain a free and open society. Hotels themselves have to be accessible. They have to have, certainly, elements of security, but they don't want to look like armed camps. We understand that. So it is a big challenge in a free and open society.

But as I say, I am really speaking for New York. We believe that we are doing everything that we reasonably can do, given the resources that we have, and certainly working closely with our Federal partners.

Ms. JACKSON LEE. Planning is extremely important.

Mr. McJunkin, in the course of the testimony of witnesses that we have heard, the use of the word commandos versus suicide bombing. Would you comment on what you think the increase of that tactic may be, such as the commandos, and your assessment of whether or not we continue to be vulnerable in sectors like hotels, resort areas where we are close to water?

Mr. MCJUNKIN. Madam Chairwoman, I would say that we are always vulnerable, and these types of attacks continue to mature. They also change tactics to thwart our efforts, and they will continue to find any means necessary within their capabilities to hit us. I believe that that is in fact true.

I also would say that, within the United States, we have, within the FBI, 56 field offices, over 61 legal attaches overseas; 100 JTTF or JTTF annexes working Nation-wide on this problem full-time. We are assertive in our approach, and we conduct on-going investigations. Beyond the State and local, the FBI and our partners have teamed up with more closely than ever with our intelligence community partners in order to spot and assess potential threats before they ever enter our shores. We work with the Department of Homeland Security to make sure that we have TRIPwires in place to identify those people as they come into the United States. We also look, on the local and State departments, my experience is that we have come a long way. Those departments have greatly enhanced their capabilities. They are constantly vigilant, and they haven't lost the scent. We are encouraged by that.

I would say that we have vulnerabilities, and it would depend on the part of the country that we are talking about as far as resources and training and all of that that rolls in. But I am still encouraged by our improvements and our continuing working relationships.

Ms. JACKSON LEE. This is my last quick question to Mr. Snyder, and it has to do with information. I have tasked the subcommittee staff with looking into DHS coordination efforts with the private sector, very important. But I was troubled to hear that information about mitigation measures was not posted on the Homeland Security Information Network for nearly a week following the Mumbai attack. Could you please explain, in light of the fact that similar information was provided to the law enforcement network, TRIPwire, which is good, the day following the attack, following this, have you made improvements so that the information and outreach can get to its needed source as quickly as possible?

Mr. SNYDER. Thank you, ma'am. The system that we used or the process we used for Mumbai was on the Wednesday evening, the 26th, as the attack began, basically, we posted on HSIN–CS existing products that had dealt with the common vulnerabilities, the potential indicators of terrorist attack, and the protective measures that had been developed generically for hotels, as well as rail stations previously. Then, as you mentioned, TRIPwire, we posted on the 27th, Thanksgiving Thursday, some information that was beginning to come out of the law enforcement channels related to Mumbai as the attack unfolded. We updated that a couple of times on TRIPwire, and at that point, we were beginning a process to integrate TRIPwire with HSIN–CS, but we did not yet have it to the point where we had tear lines to remove the law enforcement sensitive information from the information available to go out to HSIN–CS on the FOUO level. So, first thing Monday, with the new things out of the TRIPwire development over the weekend, we did the tear line posting of updated common vulnerabilities, potential indicators, and protective measures to HSIN–CS.

Now, since then, we have linked those two things together so that you actually see, the products are developed with that tear line information, and you see it almost seamlessly from one to the other.

Ms. JACKSON LEE. Well, thank you. I know that that is something that we need to further review.

Let me now recognize the gentleman from Pennsylvania, Mr. Dent, for 5 minutes.

Mr. DENT. Thank you, Madam Chairwoman.

Commissioner Kelly, I just wanted to just raise a question for you. Obviously, many of the people on this committee and elsewhere are certainly very concerned about terrorist attacks, and we have observed over the years that al Qaeda has looked to attack great American symbols, whether they be the World Trade Center or the Pentagon or wherever else they may be planning. That said, you have talked about the Mumbai attack as a turning point, and that the other groups could mirror the relative simplicity of that type of attack on perhaps a soft target like a hotel, which you talked about. Could you expound a little bit about that and what

your views are about New York and perhaps other communities, the type of threat that is posed to us by terrorists on softer targets?

Mr. KELLY. Well, we have seen a change from the patterns that have developed with Mumbai and Lahore, as we said, in groups of well-trained, small number of, relatively small, 10 or 12, armed with fairly basic weapons. Our folks who went to Mumbai don't believe that the weapons were even automatic, that they were semi-automatic hand guns. Yet they killed and wounded almost 500 people. They were well trained. They were armed with hand grenades. They were armed with improvised explosive devices. So we don't want to put ourselves in a corner. We want to be flexible in our planning and flexible in our ability to respond to any contingency.

The concern that developed with Mumbai was the fact that you might have multiple sustained events happening in the city at one time. So we have responded by increasing, as I said in my remarks, the number of people trained to sort of back up our heavy weapons first responders, which are emergency service units. There is a cadre of 400 officers that do that. We spend a lot of effort in training them. We are now expanding that to a goal of having 1,500 officers who will be able to back them up, so to speak, and be sufficiently trained in both the use of weapons and tactics to help us in a sustained attack. So we are gaming these sorts of thing. We have table-top exercises. We just had one last Friday for our commanders and a similar fact pattern and that is what we believe is going to help us respond if, in fact, there is an event such as Mumbai in New York City.

Mr. DENT. Also mention, too, that it seems that New York and Mumbai share some striking similarities in that both are financial centers of their countries, both are accessible by sea, and both are premier terrorist targets. I guess what I want to know is that the perpetrators of the attacks in Mumbai entered the country via the ocean, I believe. How would you describe the New York Police Department's relationship with the U.S. Coast Guard? How confident are you that a suspicious vessel entering New York Harbor would be detected?

Mr. KELLY. Well, we have an excellent working relationship with the Coast Guard. We have personnel assigned to their operational headquarters in New York City. The members of our Harbor Unit, which is our maritime unit, are cross-designated by the Coast Guard so that they are able to board ships. We have exercises on a regular basis. When an event happens on the waterways, we frequently have a joint response. So I believe we have a very high level of cooperation and camaraderie with the Coast Guard.

Mr. DENT. Well, I am glad to hear that. I guess my final question before I run out of team here is this: You mentioned during your remarks that you have been reaching out to hotel owners trying to work with them about the various threats that they may face. How seriously do you think that these hotel owners and others are taking the recommendations that you are providing to them? Are they taking these tips seriously? Are they training their staff appropriately? Do you think they are engaged enough?

Mr. KELLY. I think they are taking it very seriously. We have had a strong working relationship with them for quite a while. Under the NYPD Shield rubric it has only gotten stronger. As I

said, we have a special unit now that just works with hotels. They are, you know, they are concerned, and they are serious about investing in training for their staffs and investing to the extent they can to sort of harden the target without, you know, making it look like an armed camp. So they are very much engaged in this issue.

Mr. DENT. Thank you.

I thank you all for your service.

Yield back my time.

Ms. JACKSON LEE. I thank the gentleman.

The Chair will now recognize other Members for questions they may wish to ask the witnesses. In accordance with our committee rules and practice, I will recognize Members who were present at the start of the hearing based on seniority on the subcommittee, alternating between majority and minority. Those Members coming later will be recognized in the order of their arrival. I would like to get to as many Members as possible and ask them to also return after the last votes of the day.

The Chair recognizes for 5 minutes the distinguished gentleman from Mississippi, the Chair of the full committee, Mr. Thompson.

Mr. THOMPSON. Thank you, Madam Chairwoman.

Deputy Assistant Secretary Snyder, did DHS produce any recommendations after the Mumbai incident?

Mr. SNYDER. Yes, sir. We did produce through the TRIPwire and out through the law enforcement community, as well as posting on HSIN–CS a couple of pieces on the specific tactics, techniques, and procedures used by the terrorists in Mumbai and the potential protective measures that might be taken by the facilities to become aware of something like that, raise their security files.

Mr. THOMPSON. Were these advisory in nature? Or have we established some policy?

Mr. SNYDER. They are always advisory in nature, due to the partnership framework and the 85 percent of the critical infrastructure that is owned and operated by the private sector. The tactical level of that is the vulnerability assessments and the recommended actions provided by the protective security advisers, when they visit the actual facilities in the field, the high-risk facilities. But what we try to do is analyze what went on and then advise those partners on the actions they might take. Many of them are things that you would think of, such as surveillance cameras, such as you mentioned, training.

Mr. THOMPSON. Thank you. Can you provide the committee with whatever recommendations the Department provided, whether they were advisory or whatever, after Mumbai?

Mr. SNYDER. Yes, sir.

Mr. THOMPSON. Commissioner Kelly, I know you work with New York. When your teams go out working with hotels or whomever, is the protocol to make suggestions as to how they can do better if it is an existing structure, or is there some protocol established through the city for new construction that would be a little more than advisory?

Mr. KELLY. No, it is right now, at this time, advisory. There has been some discussion about putting forward best practices, as far as construction is concerned, the actual construction of buildings. Of course the Building Code itself has been somewhat upgraded,

perhaps it needs to be, some of my staff believes it needs to be upgraded even more.

But since September 11, there have been upgrades in the Building Code. But to answer your question specifically, when we work with our hotel management, for instance, we are strictly in an advisory capacity. There are not too many hotels that look exactly alike, certainly in New York. So we make suggestions, make recommendations, but they have to adapt them to their own situation, their own structure.

Mr. THOMPSON. To the extent, Deputy Secretary Snyder, how many other cities would you say are as prepared for these situations as New York?

Mr. SNYDER. Well, certainly, you know, I think you will find or what we have found through our coordination with these associations and our sector councils and subcouncils that deal with the hotel and resort industry, you will find areas that are highly populated, resort areas or highly populated cities with a hotel industry that is pretty robust, you will find, you know, quite a bit of preparedness and an awareness of measures that go on routinely about training personnel what to look for and so forth, when you, and of course——

Mr. THOMPSON. I just need a number.

Mr. SNYDER. Oh yes, sir. Oh the number of cities? Certainly there is——

Mr. THOMPSON. Name, number.

Mr. SNYDER. The top five, you know, New York, Washington, Chicago, Los Angeles.

Mr. THOMPSON. So you are comfortable that those cities meet some standard that your Department is comfortable with.

Mr. SNYDER. Well, as Commissioner Kelly said, there is not a specific standard that exists right now. As I touched on during my opening testimony, there is this potential for the voluntary private-sector standards. That has some promise in it, that will balance.

Mr. THOMPSON. Madam Chairwoman, I yield.

Ms. JACKSON LEE. Obviously, the Chairman has raised questions about preparedness, and certainly five cities out of what I think may be thousands in this country leads us to believe we have some important questions to ask.

I would ask now that the witnesses, if they would, would wait on our return. We will recess the committee for votes, and we will return immediately. This committee is now recessed.

[Recess.]

Ms. JACKSON LEE. The meeting will come to order.

Mr. King, if you would indulge the witness from the FBI who indicated to staff that he had not completed his answer on the tactics question. Once he completes, I will yield to the distinguished gentleman from New York.

Mr. McJunkin, would you finish your answer, please.

Mr. MCJUNKIN. Thank you, Madam Chairwoman.

I just wanted to expand on one point. It was something that was addressed in Commissioner Kelly's earlier testimony to the Senate, and it addresses your point to Mr. Dent's earlier question as well.

We have seen similar tactics in prior investigations here in the domestic United States. In fact, there are three that come right off

the top of my head: one in Los Angeles, one in Chicago, and one more recently in Fort Dix, New Jersey, where those individuals had similar types of weaponry, similar types of planning and plotting, similar types of targeting.

We had Jewish synagogues in Los Angeles as well as military recruiting stations, shopping mall in Chicago, and then in Fort Dix, it was the military installation there.

I would like to point out that these things don't occur by accident. It is the close working relationship that we enjoy of cross-agencies, Federal, State, and local, Department of Homeland Security, certainly the New York City Police Department, and our agency as well where we take advantage of each other's resources, we take advantage of each other's time, and we are able to thwart these efforts before they take route.

That is the conclusion of my statement, ma'am.

Ms. JACKSON LEE. Let me thank you.

At this time, I will recognize the gentleman from New York, Mr. King, for 5 minutes, the Ranking Member of the full committee.

Mr. KING. Thank you, Madam Chairwoman.

I would like to address my questions to Commissioner Kelly.

Assuming the worse, assume there is an attack on a New York hotel similar to Mumbai. Do you feel confident that you would have immediate contact with the hotel security, and they would be responsive to you, and you would be on the same page, the same wave-length?

Mr. KELLY. That is certainly our goal. That is what we are training for, and yes, I feel reasonably confident, given our activities of the last few months, that we would be able to work closely, contact them very quickly and work closely with them if a similar event happened.

Mr. KING. Are most of those security directors retired law enforcement?

Mr. KELLY. Many of them are. Sometimes a big change will bring people in from other areas of the country who not necessarily are law enforcement, but there is also kind of a homegrown cadre of former law enforcement people and are in charge of securing the hotels.

Mr. KING. Assuming there was an overlap between the hotel and transit system, how closely coordinated are you with the MTA police or the Port Authority police? What I am looking for is the level of cooperation in those first few minutes or hours.

Mr. KELLY. I think the level of cooperation in those instances would also be very high. We work within the port authority. Obviously we have interactions on a daily basis. The port authority is on the Joint Terrorist Task Force, the MTA police representative as well. So that is another venue when you would come together.

The MTA police chief, Michael Coan, less than a year ago left the NYPD. He was a chief in the NYPD. He is now chief of the MTA police. We have a close relationship.

Bill Morange is the executive vice president and security is under his bailiwick. He is a former NYPD chief. So just on a person-to-person basis, we have a good working relationship. But operationally, we have a good working relationship.

Mr. KING. How about FBI and Homeland Security?

Mr. KELLY. We have an excellent working relationship. We—over 120 of our detectives working with the FBI and the Joint Terrorist Task Force. Homeland Security, we have the contacts on a daily basis. I was just talking to the general about Securing the Cities program that we have been involved in Homeland Security for the last 2 years. That is a program where state-of-the-art radiation detection equipment is being distributed to an area, in essence, a 50-mile radius from New York City. That is going extremely well. Homeland Security is helping us with our Lower Manhattan Security Initiative.

So I think we have excellent cooperation and daily interaction with both agencies.

Mr. KING. If a hotel or a transit system is attacked, basically, all you can do is minimize the damage and fight back. I think you have always taken the approach of having to layer defenses, of knowing in advance. That is why you have the 11 police overseas to get intelligence, why you have the Secure the Cities to detect radiation devices coming into the city.

How important is intelligence both overseas and what you get from the Federal Government, and how vital do you believe the Secure the Cities program is going to be as far as building up those layers of defense? Mr. Lungren is always talking about layers of defense. There is no silver bullet that we have to have those structured layers.

Mr. KELLY. Intelligence is the key. No question about it. You want to stop them before you have to respond to an event, and intelligence is the essence of prevention. We rely on our Federal partners for our intelligence. The things that we do supplement what the Federal Government does. We certainly can't substitute. We can't do it on our own. We need a strong Federal partnership. So intelligence is, in essence, coming from Federal resources.

It is probably the most important element of them all. We get information that enables all of our agencies to intercept, to prevent before we have to be a first responder. It is key.

Securing the Cities is, as I said, a very important initiative. We are the first city in the country to have this program. The Homeland Security has been extremely supportive in that regard. It is well on its way, and the concept is to have, as I say, sort of concentric rings of radiation detection equipment starting approximately 50 miles away from the city but certainly right into the heart of the city itself and of all of the tunnel and bridge entrances going into Manhattan. That program is progressing well.

Mr. KING. Thank you.

Ms. JACKSON LEE. Now I will recognize Congresswoman Titus for 5 minutes.

Ms. TITUS. Thank you, Madam Chairwoman, and thank you for having this hearing on a topic that is very important to me.

I represent parts of Las Vegas where we have dozens of hotel casinos with some of the most top-notch security technology and personnel in the private sector. I am sure you have all heard of the eye in the sky that watches you on the casino floor, and if you saw Oceans 11, it is not far wrong.

So I would direct my question to Mr. Snyder and invite the rest of you to comment, too.

I am glad to hear that you have so many planning and assessment programs in place. I think I counted 13 acronyms in two paragraphs. They range from the BZPP to the C/ACAMS. But what troubles me a bit is in your statement you say, for example, during the Mumbai event, the PSA for Las Vegas met with hotel, casino, and resort security officials to answer questions and distribute our CVPIPM reports that provide details on enhanced security recommendations and best practices.

Now, the reason that bothers me is that it seems to suggest it is kind of late in the game that they are getting this information about best practices and recommendations, and secondarily, if they are getting it, that means they haven't been involved in the process. So we are not taking advantage of all of the assets that they have already in place.

So could you tell us, and in kind of layman's terms, what is going on with all of the hotels in Las Vegas, and if we could find a way to take better advantage of that security system that is so incredible already.

Mr. SNYDER. Well, I would, ma'am, want to make sure that that wasn't the only perception of what I provided in the statement.

The reason that they were calling the PSA is that there was already a relationship established through prior associations. I don't it have exactly in front of me, but the regular engagement between the PSA, for instance, there has been over 100 liaisons and outreach visits in the lodging sector, but they are continuously engaged, particularly in the Los Angeles or the Las Vegas area because of the mass of the activities there of high value and the State Homeland Security adviser, the State police, the Las Vegas Metropolitan Police Department, State Gaming Commission representatives and corporate security managers.

So there are regular meetings there with all of those partners and the protective security adviser, as well as members from the Department level that come down to do either table-top exercises or assessments.

So that relationship is a strong one, and certainly we took advantage of that at Mumbai, and they called the PSA and we pushed out that information.

Ms. TITUS. Any other comments?

Mr. KELLY. I really have nothing to add. I am focused, of course, on New York. I think it is safe to assume that hotels in New York don't have that level of technology that exists in Los Angeles. But the people I talked to are very aware of technology in the hotel.

So I really have nothing to add.

Ms. TITUS. Thank you, Madam Chairwoman.

Ms. JACKSON LEE. I can assure you being on this committee, help is on the way.

We thank our witness.

I now yield 5 minutes to the gentleman from California, Mr. Lungren.

Mr. LUNGREN. Commissioner Kelly, now do I understand it right that you went to a Catholic grade school called St. Therese?

Mr. KELLY. Yes, sir. I did.

Mr. LUNGREN. I was told by Mr. King that he followed you by 2 years and beat every one of your academic records; is that right?

Mr. KELLY. That was easy. I am sure he did.

Mr. LUNGREN. It just shows you how someone can rise to a position of prominence and other people are stuck where Mr. King is.

Commissioner Kelly, in your written testimony, you talk about your Department's analysis of the attacks that took place in Pakistan and the fact that your Department has three liaison offices overseas.

Some people have suggested that you folks ought not to be in that, that is the business of the Federal Government, the FBI, the CIA, the operatives that we have. Some have said you are not the FBI and that you may have gone too far. Now, I don't know what they meant by that, but I would like to hear from you why your Department thought it was necessary and how you, I presume, feel that that is value added to whatever your Department would normally do domestically and value added to what you get from the FBI, the Federal Government, or any other links that you have to other agencies.

Mr. KELLY. I sit in a building that is five blocks away from the World Trade Center. I live a block away from the World Trade Center where almost 3,000 people were killed. I was police commissioner in 1993 when we had 1,000 people injured at the World Trade Center site. No other U.S. city has suffered the losses that New York City has. We have had six plots against New York since September 11. So we see ourselves as top of the target list, and I think that is supported by a consensus of people in the intelligence community.

We are looking for any bit of information that can better protect our city. That is what our overseas liaisons give us. We were able to get real-time information. As a matter of fact, I was talking to our officer in an operation center at new Scotland Yard on July 7, 2005 when the subway attacks took place. Obviously, that happened during their rush hour. New Yorkers getting on the subway 5 hours later would be concerned. We wanted to raise their comfort label and enable us to deploy additional resources, I think, to ease that concern that people have.

So it gives us real-time information about what is happening overseas.

Now, I must also tell you that taxpayer money is not funding the cost of these officers overseas. It is funded by private foundation. Salaries are paid by public funds, their expenses are paid by a foundation.

But we think it is value-added. We are able to get information quickly. We got information very quickly about the Madrid bombings that took place in March 2004. We just see ourselves as being positioned differently than other U.S. cities.

Mr. LUNGREN. I am from the West Coast, for instance. Used to be from Long Beach, I am now from Sacramento. But if I am one of those departments, do I have a relationship with your department so that I can get information on a timely basis, or would that be a mistake if you had to respond to all other departments?

What I am saying is you have actionable information, you believe you get it in a timely fashion, you take certain steps based on that. Some of that information might be a benefit to your brethren in other departments. Is there a means, a mechanism by which you

share that information, or does that go through the Feds or how does that happen?

Mr. KELLY. I mean, logically, if there was a threat against Long Beach, we would notify the Long Beach authorities.

But the natural vehicle for the information is through the Joint Terrorist Task Force. That is the entity that has the broadest reach and the quickest reach as far as disseminating information of that type.

Mr. LUNGREN. So what I am getting at is if you have information through your chain of command, as opposed to DHS or FBI or so forth, and then you thought it may not be specific to Long Beach or specific to Sacramento but it would be of interest to them, would you share that through the joint task force; is that how you would do it?

Mr. KELLY. Absolutely. The information sharing has never been better. There is a concern, really, years ago, about the lack of information sharing. I think that is ancient history. Now, the information exchange and information sharing has never been better.

Mr. LUNGREN. Could I ask you, with the indulgence of the Chair, with respect to the attack in Mumbai or the attack in Pakistan, were you satisfied with the timeliness of the information that you received from the National Terrorism Center or the Department's national operations center?

Mr. KELLY. You know, we always want a little more. I think we get probably——

Mr. LUNGREN. I understand that, but we are trying to figure out—I am not trying to point fingers at anybody.

Mr. KELLY. We are not taking away from anybody. I think you have to understand, this is—we are supplementing. This is value-added.

Mr. LUNGREN. My question was were you satisfied with the timeliness of the information that you received from the National Terrorism Center, Counterterrorism Center, or the National Operations Center?

Mr. KELLY. We didn't get the depth of the information from the national assets in a timely fashion like we were able to get from our own people.

As I said, on December 5 not only, you know, our own people, we obviously use it in-house, but we had a meeting of security directors in New York City, had 400 of them in our auditorium on December 5. The attacks happened November 26 and November 29. On December 5, we had 400 people there. We had independent information, and we had our team in Mumbai on a telephone hook-up with pictures that they had taken giving them specific information.

So that is why I say it is value-added, it is something more. That is what we feel that we have to do given the history of New York City. We want that leg up.

Ms. JACKSON LEE. The gentleman's time has expired.

I recognize now the distinguished gentleman from Missouri, Mr. Cleaver.

Mr. CLEAVER. Thank you, Madam Chairwoman.

Let me apologize to the panel. I would like to come and stay to the end, but I have a Financial Services Committee hearing going

on at the same time. But this is extremely important, and I am very much concerned about what I consider to be the inevitability of such strikes as Mumbai because while I guess we can't categorize the hoodlums as terrorists who were coming in with explosives tied to their bodies, I think, at least based on what I read, they came realizing they would not get out alive.

Am I on the right track that when terrorist groups decide that they will sacrifice their life or their lives, that it is difficult for us to stop it? I mean, there are preventative steps we can take, but I mean, what I think people say quite often and you hear on television, "We want this never to happen again." I want to know about the impracticality of such a statement based on what happened in Mumbai.

Mr. McJunkin.

Mr. MCJUNKIN. Yes, sir. I believe that the—I learned from an AUSA in Texas that people move through time and space, and when they do, they leave clues. In that, our ability to thwart such attacks, regardless of the determination of the individual attacker, it comes from our ability to share information effectively and to be cognizant of the threat and to be assertive in our searching of clues that will allow us to bring them, dismantle them, and disrupt them before they have an opportunity to strike.

I think that the important takeaway here is that any group, no matter what their intent is or what their target is, has to obtain a certain level of capability. It is our job, DHS's, the FBI certainly, and the New York City police, as well as every other police department in the United States, to be attuned to the clues that we learned, particularly to attacks occurring overseas, and look at them in the United States.

It could be a police officer that is answering a domestic call that notices a strange odor in an apartment near by the call. It is incumbent upon that officer to knock on that door and find out what that smell emanates from. It is clues like that that allows us to attack their capability.

We also have to be with the private sector. It has been brought up here a number of times today that the private sector has to be engaged. That is never truer than it is today. It is those corporations and companies through their normal business protocols and processes that will just in the normal course of business stumble onto the clues that if we have an effective sharing operation amongst ourselves and them, we will be able to provide the links that give us that opportunity to disrupt their ability to build capability.

Mr. CLEAVER. Which is comforting, brings some comfort.

I guess maybe the answer I am looking for probably might not bring comfort, which is these were suicidal terrorists. I mean, they went in without any expectations of leaving, they didn't have bombs strapped to their bodies; but they realized at one point they were not going to get out alive. I guess my question is, and maybe I asked poorly the first time, is: Isn't it infinitely, for us, more difficult for us to say to the public things like "this will never happen again," when we realize that if people are willing to sacrifice their lives, they can kill others?

Mr. MCJUNKIN. Sir, yes. I would agree with you.

I think that we are—in these times, we have to accept that reality and understand that and determined people will, in fact, be able to successfully accomplish their missions. Our job is to make sure that we minimize that before and after they begin their quest.

Mr. CLEAVER. To any of the three of you, is there anything that we need to do legislatively to equip all of the agencies involved, including Homeland Security, to do it just as you said, minimize the likelihood of such an event here on our shores?

Mr. SNYDER. I would just say certainly the continued support of the committee is very helpful to us at the Department, particularly infrastructure protection with the private sector; specifically, being able to continue to develop these operational relationships so we can have a deterrent effect in time in advance and doing the training and the exercises that we do is very helpful in trying to prevent what you are talking about.

So we want to continue that work.

Ms. JACKSON LEE. I thank you, Congressman.

I am pleased to yield 5 minutes to the gentlelady from Arizona, Ms. Kirkpatrick. Welcome. Thank you very much.

Ms. KIRKPATRICK. Thank you. I represent a vast rural district in Arizona, and it includes ranches, right along the border between Arizona and Mexico, it includes agriculture, farming, and also rural electric co-ops which are sort of the energy center for the district.

What kinds of things do you have in place to let them know, to communicate, to share information specific to those groups?

Mr. SNYDER. Well, we do, in our sector coordinating councils partner with the Department of Energy to reach the energy industry, including the rural electric co-ops, so that these, similar to the hotel industry, the dialogs, the preventative measures, those things that are developed, the risk assessments not only happens at the strategic level, at the Federal, national level, but they also take place down in the local levels and get passed down, communicated, passed down by the sector coordinating councils, the associations that are members of that and corporations and all of the cooperatives that belong to a larger corporation.

So they participate in that same level of interest and of preparation and of risk assessment, vulnerability assessment on their facilities.

So we think that they are engaged at that level and know what their vulnerabilities are and what their preparatory actions might be. They also, I am sure, are linked with their local law enforcement for response measures.

Ms. KIRKPATRICK. Interoperability in our district is a huge problem, and I am a former prosecutor so I have been in talking with law enforcement agencies. They can't yet communicate seamlessly with each other let alone with many of these communities.

So what is being done specifically to bolster that system so that there can be continuous communication, and especially in an emergency?

Mr. SNYDER. I do know there is specific work being done on the interoperability issue, and I am personally not versed enough in it to offer an answer here, but I will be happy to get back to you with information on those, some of which are in the science and technology area.

Ms. KIRKPATRICK. I yield back my time.

Ms. JACKSON LEE. I thank the gentlelady very much. Let me prepare the witnesses as we move to the next panel to just clarify the record through Commissioner Kelly for a very brief moment to ask a question that seems to need clarifying.

Commissioner Kelly, I think in your testimony—and you can just, if you would, clarify it—that either in your research or the visits of your officers glean that these commandos did not intend to commit suicide; they intended to survive; is that correct?

Mr. KELLY. I believe it is not all——

Ms. JACKSON LEE. They were not suicide bombers.

Mr. KELLY. I believe there are still questions in the intelligence community as to whether or not the Mumbai attackers initially decided to or had a mission to kill a lot of people and then die. It was some belief that it may have changed.

We look at the transmissions. The Indian government put out a report of the exchange of messages that took place from people in Pakistan talking to the individuals in Mumbai, and some believe that it may have just sort of moved in that direction.

If you recall when you look at the report, two individuals that are—one is captured and one is killed—they are driving past the hospital. It looks like they were driving north on the Peninsula perhaps attempting to get away. Now, we talk about the Lahore attack, of course all of those individuals escaped. None of them committed suicide.

Ms. JACKSON LEE. Thank you, Commissioner.

To follow up with you, Mr. McJunkin, because I think your testimony suggested the decentralizing of terrorism, and if not, testimony has been said today the decentralizing like LeT and others.

With that in mind, do you feel that our mechanism, DHS, FBI, and others, are moving toward understanding the potential for commando-type activities on the soil of the United States?

Mr. MCJUNKIN. Yes, ma'am. I think that our intent across the board across governmental agencies is to be ready for anything. It is tough to game plan every possible scenario. But I think we are naturally able to respond to this type of an attack just because of the way of our law enforcement is structured in the State, local, and Federal levels.

I think that our influx of intelligences and combined with the information that is coming off the street from the patrol officer allows us, the way we move information, rather than in selected sleeves that were traditionally law-enforcement based, criminal prosecution driven, ways we moved information—we have now sort of wiped those walls away and with all of the information now flows equally left and right, north and south.

So I think that advantage that we have gained since 2001 has moved the ball down the field considerably for us in the law enforcement communities.

I think we game-planned for the big scenario, the WMD. We have to have the resources and the capabilities necessary to continue to confront that threat. But I also think that our cities, particularly our States and also in the rural areas of our country, our law enforcement officers are better trained today than they have ever been. The local crime and the normal crime that they see in

these cities in these rural areas very much mirrors this type of threat.

So I think we are very well-suited to address it. It is just a matter of raising the level of awareness and making sure that we don't lose our edge.

Ms. JACKSON LEE. I am very glad that you ended on that note because Alabama, the incident over the last 20 hours, was not a terrorist act, but what it did show us was someone who is interested in doing harm can move from one jurisdiction to the next on our own soil and we have got to work with each other.

I want to thank the witnesses, Secretary Snyder, Secretary Kelly, and Assistant Director McJunkin from the FBI for giving us what I believe is vital testimony.

As I indicated, this is a question of resources, intelligence, but it is also a question possibly of enhanced legislation to sort of get our hands around the next step in fighting terrorism here and abroad. So I thank the witnesses. The witnesses are now complete with their testimony.

We now welcome our second panel to the witness table.

Our first witness, Dr. Christine Fair, is a senior political scientist with the RAND Corporation. Prior to rejoining RAND, she served as a political officer to the United Nations Assistance Mission to Afghanistan in Kabul. Dr. Fair's research focuses upon the security competition between India and Pakistan, Pakistan's internal security, the causes of terrorism in South Asia, and U.S. strategic relations with India and Pakistan. She has authored, co-authored, and co-edited several books, and recently co-authored a RAND report about the attack in Mumbai entitled "The Lessons of Mumbai."

Our second witness is Mr. Brad Bonnell. He is the director of global security at InterContinental Hotels Group, InterContinental Hotels Group includes seven hotel brands, over 160 million stays per year, almost 620,000 rooms, and more than 4,150 hotels across nearly 100 countries. As director of global security, Mr. Bonnell's primary duties include directing the corporate counterterrorism program, providing internal security services, and crisis management planning.

InterContinental Hotels Group has been involved with the real estate information sharing and analysis center in partnership with DHS, and it is aligned with the State Department's overseas security advisory council. Through its membership on the real estate round table, it is a member of DHS Commercial Facility Sector Coordinating Council. Welcome.

Our third witness is Mr. William Raisch. Mr. Raisch is the director of the International Center for Enterprise Preparedness at New York University. He founded the Center with initial funding from the Department of Homeland Security as the world's first academic research center dedicated to private sector emergency preparedness and resilience.

Directly prior to founding the Center, Mr. Raisch served as the private sector preparedness adviser to the 9/11 Commission and assisted in developing the Commission's recommendations on private sector emergency preparedness.

He continues to support the efforts of the 9/11 Public Discourse Project in its on-going reporting and advocacy activity. Mr. Raisch

is actively involved in the 9/11 Acts Voluntary Private Sector Preparedness accreditation and certification program. Established in Title 9 of the act, this program has the potential to help foster preparedness and security at the types of assets in the United States that were attacked in Mumbai.

Without objection, the witnesses' full statements will be inserted into the record.

I now ask each witness to summarize his or her statement for 5 minutes beginning with Dr. Fair.

STATEMENT OF C. CHRISTINE FAIR, SENIOR POLITICAL SCIENTIST FOR SOUTH ASIAN POLITICAL AND MILITARY AFFAIRS, RAND CORPORATION

Ms. FAIR. Thank you, Madam Chairman, and your esteemed colleagues, for the opportunity to speak about Lashkar-e-Taiba and its parent organization Jamaat ul Dawa the group that perpetrated the terrorist attack on Mumbai.

I was asked to focus on four specific areas, and I will do so briefly in term.

The first situating Lashkar-e-Taiba among Pakistan's numerous terrorist organizations. I have a much more lengthy written statement that really distinguishes Lashkar from the other groups but also shows how it resembles other groups in many important ways. But I would like to make the following points here.

First and foremost, Pakistan has used militancy as a tool of foreign policy since 1947. With very few exceptions, Pakistan's militant groups enjoy, enjoyed, and likely will enjoy state patronage including financial, military, and other assistance. Among these groups, Lashkar-e-Taiba is the most lethal. LeT differs from the numerous other groups operating in Pakistan in that its ideologies are actually Ahl-e-Hadith. The other groups are actually Deobandi, and the Deobandi groups include the Afghan Taliban, the Pakistan Taliban, etc.

What this means is there are important ideological differences despite similarity of rules.

Now, Pakistan frequently points out that it is, itself, a victim of terrorism, and it surely is. But I would like to point out that the groups targeting Pakistan has been Deobandi. Lashkar-e-Taiba has never attacked a target, either state or international, within Pakistan itself; and as of yet, there is no credible evidence linking the attack on the Sri Lankan Cricket Team to Lashkar-e-Taiba. This fact has led many analysts to believe that Lashkar-e-Taiba has continued to enjoy state support in various guises despite the state's recent efforts to ban that organization, actually the parent organization.

Turning to its origins, operatives, and operations, I would like to point out that we may just be hearing about it now in 2008, but it has been around since 1986. It was founded by two engineering professors along with Abdullah Azan, a close associate of bin Laden. Its parent organization was actually set up to fight in Afghanistan and it set up its own camps to do so. It became operational in the Indian Kashmir in 1990. I have been perusing LeT literature now for years since I was a graduate student, and going back to the 1990's, you can see in their literature and in their post-

ers a very clear desire to target Indians, especially Hindus, Jews, Americans, and other infidels and apostate Muslims.

They have been long interested in stoking larger Hindu-Muslim discord in India and liberating all of India in establishing a caliphate there.

MDI which is its parents organization, Lashkar-e-Taiba, they claim to have participated in a number of national jihads since their setup in 1986. Most of these can't be independently confirmed. However, what we do know is that LeT-associated individuals have appeared in Iraq, Australia, the United States, United Kingdom and numerous European cities and Lashkar-e-Taiba attacks U.S., NATO and Afghan allies in Afghanistan.

LeT has a hallmark modus operandi. It is not suicide attacks, as we have heard. Rather they are high-risk commando-style missions. They always pick missions in which there is a slim chance that they will survive. But the preference is to be killed killing as many people as possible rather than being taken hostage or taken captive by the authorities. The reason for that is very clear as we have seen from the loan surviving gunman: once captured you talk.

So the preference is to kill as many people as possible before you yourself are killed.

I would like to point out that this particular style of Fidayeen attack is also not new in the Lashkar-e-Taiba repertoire. They have in fact been doing this since 1999. They first attacked outside of Kashmir in 2000 when they did a Fidayeen attack on the Red Fort in New Delhi.

Turning to the third section, the antecedents and innovations of the Mumbai attack, in many ways that attack resembled other attacks perpetrated by LeT. What differed, of course, was the scope and the number of targets. LeT has actually long pioneered the use of sea routes to get explosives and personnel into theater. Certainly, this particular attack pushed the use of sea routes farther than it had ever used before. The sea routes and other logistical networks that Lashkar has been able to build in India has actually been very important. Lashkar's been operating outside of Kashmir against since the late 1990's, and to do they rely upon international networks, such as those based in Bangladesh. They also rely upon domestic Indian collaborators as well.

When I look at the Mumbai attack, two elements strike me apart from the number of targets involved.

First is that even though they have been attacking U.S. soldiers in Afghanistan since at least 2007, maybe earlier, this is the first time, despite a dedicated rhetoric of attacking Americans and other internationals, that they have actually done so.

The second interesting target was the Chabad House. Lashkar has always been deeply anti-Semitic, but I would like to point out Mumbai has a very historical Jewish community. In fact, India has a number of Jewish communities. Yet despite the decades of Islamists and avowedly anti-Semitic militant groups attacking within the Indian homeland, never before has an Indian-Jewish target ever been assaulted. So Chabad is not simply Jewish in the Lashkar-e-Taiba targeting logic. It is explicitly Israeli. We now know from the intercept of phone conversations it wasn't simply anti-Semitism, it also had the additional value of disrupting the

important India-Israeli security intelligence relationship that has developed in recent years.

So very briefly in conclusion, I think the question that we all have is whether or not Lashkar-e-Taiba can undertake such operations in the United States. I am going to give a firm "maybe." There is never a penalty for exaggerating a threat, but if you underestimate it, you get dinged.

There have been a number of individuals, including converts who have radicalized in the Diaspora and who have traveled to Pakistan to train with the Lashkar-e-Taiba and other militant groups, such as Jaish-e-Mohammad. Lashkar-e-Taiba and other militant groups in the Pakistani province of the Punjab comprise an important link between those who have radicalized in the Diaspora and elsewhere in Pakistan's tribal area where al Qaeda is firmly ensconced.

During my recent trip to Pakistan a week and a half ago, one of my interlocutors described these Punjabi groups as the escalator that connects the foreign militants to the tribal areas.

Given the difficulty in Pakistan-based operatives in obtaining a visa to come to western countries, the strategy of pulling people in from the West is likely to be the most productive strategy as those individuals likely speak English, have the appropriate passport, they are more able to gain access to the targeted countries, and especially those with the visa waiver program are countries of origins that are of considerable concern.

Thus to conclude, LeT certainly poses a number of concerns for the United States, not the least of which include LeT-supported cells attacking U.S. assets, citizens, etc., either at home or abroad, on-going operations against the United States and its allies in Afghanistan, the likelihood of future attacks in India with the ever-present possibility of prompting yet another Indo-Pakistan military crisis.

For these and other reasons, it is absolutely imperative that Washington insists that Pakistan not only ceases all forms of active and passive support for Lashkar-e-Taiba and similar groups, but, in fact, actively undertake efforts to eliminate them.

Ms. JACKSON LEE. Thank you.

[The statement of Ms. Fair follows:]

PREPARED STATEMENT OF C. CHRISTINE FAIR,[1] THE RAND CORPORATION

ANTECEDENTS AND IMPLICATIONS OF THE NOVEMBER 2008 LASHKAR-E-TAIBA (LET) ATTACK UPON SEVERAL TARGETS IN THE INDIAN MEGA-CITY OF MUMBAI[2 3]

MARCH 11, 2009

INTRODUCTION

On November 23, 2008 ten Pakistani terrorists associated with Lashkar-e-Taiba (LeT)/Jamaat ul Dawa (JuD), operating in four attack teams, rampaged across some ten different targets in the Indian port city of Mumbai. In part due to the complexities of the counterterrorist operations, the tenacity and training of the attackers, and the inadequate capabilities of the Indian security forces, it took some 4 days to end the terrorist campaign which claimed the lives of at least 172 victims.

In this testimony, I have been asked to focus upon four specific concerns emerging from this attack and its perpetrators. First, I contextualize LeT among the proliferating expanse of militant groups operating in and from Pakistan. Second, I provide specific information about LeT, the militant group responsible for this and many other attacks within India. Third, I draw out both the antecedents and innovations of the 2008 Mumbai attack. I conclude with a discussion of some of the important implications that emerge from this and other LeT activities for regional and international security generally and U.S. security in particular.

While LeT was banned in 2002, the LeT began operating under the banner of JuD, which was overtly operational until the Pakistan government formally banned it following immense international pressure in late 2008, including a resolution in the U.N. Security Council that JuD is a terrorist organization. In the service of brevity, I use LeT and JuD somewhat synonymously even though there are a few important technical differences.[4]

PAKISTAN'S MYRIAD MILITANTS: SITUATING LASHKAR-E-TAIBA

Pakistan has given rise to numerous militant groups in recent decades that operate to secure Pakistan's state interests in India and Afghanistan. In addition, Pakistan has sustained numerous covert operations campaigns in Indian-administered Kashmir since 1947.[5] Many—if not most—of these militant groups have enjoyed the specific patronage of the Pakistani state intelligence and military agencies to prosecute Islamabad's interests in India (with particular focus upon Kashmir) and Afghanistan.[6] These varied militant groups, until circa 2002, could largely be

[1] The opinions and conclusions expressed in this testimony are the author's alone and should not be interpreted as representing those of RAND or any of the sponsors of its research. This product is part of the RAND Corporation testimony series. RAND testimonies record testimony presented by RAND associates to Federal, State, or local legislative committees; government-appointed commissions and panels; and private review and oversight bodies. The RAND Corporation is a nonprofit research organization providing objective analysis and effective solutions that address the challenges facing the public and private sectors around the world. RAND's publications do not necessarily reflect the opinions of its research clients and sponsors.

[2] This testimony is available for free download at *http://www.rand.org/pubs/testimonies/CT320/*.

[3] The author is grateful to Peter Chalk, Lisa Curtis, James Dobbins, and Praveen Swami who reviewed earlier drafts of this testimony.

[4] Technically, LeT remained the militant wing while JuD engaged in a wider array of charitable activities such as establishing hospitals, clinics, schools, and madrassah and other poverty relief activities. Since LeT was outlawed, it largely operated under the umbrella of JuD. Proponents of JuD's innocence assert the separation of the organizations.

[5] In their most maximal objectives, these campaigns have aimed to wrest from New Delhi the portion of Kashmir which it administers. (India controls about two-thirds of the collective area known as Jammu and Kashmir.) These campaigns have sought to secure Pakistani sovereignty over the expanse of the disputed territory. In their most minimalist objectives, these campaigns have sought to "bleed India" by requiring it sustain a large (often locally resented) counter-insurgency grid in Jammu and Kashmir. For a discussion of the various covert campaigns, see Praveen Swami. *Indian Pakistan and the Secret Jihad: The Covert War in Kashmir,* 1947–2004 (London: Routledge, 2006).

[6] Ashley J. Tellis writes on this point that "In fact, of all the Pakistani-sponsored Deobandi [sic] terrorist groups operating against India in Kashmir and elsewhere, only one entity—the Hizbul Mujahideen—began life as an indigenous Kashmiri insurgent group; the others, including the most violent organizations such as the Lashkar-e-Toiba, the Jaish-e-Muhammad, and the Harkat-ul-Mujahideen, are all led, manned, and financed by native Pakistanis." See Ashley J. Tellis, *Pakistan and the War on Terror Conflicted Goals, Compromised Performance* (Washington, DC: CEIP, 2008), p. 5. Also see among numerous other sources Ahmed Rashid, *Descent*

Continued

disaggregated according to religious ideology (school of Islamic thought) and operational goals.[7]

Among Pakistan's various Islamic interpretative schools, the Deobandi school of thought claims the most militant groups. Key Deobandi militant groups include the Taliban (Afghan and the Pakistani), Jaish-e-Mohammad (JM), Harkat-ul-Jihad-Islami (HUJI), Harkat-ul-Ansar/Harkat-ul-Mujahideen (HUA/HUM), Lashkar-e-Jhangvi (LeJ) and Sipah-e-Sahaba-e-Pakistan (SSP) among numerous offshoots. The Deobandi tradition emerged as a puritanical movement to uplift Muslims by purifying Islamic practice through discouraging mystical beliefs such as intercession by saints and veneration of graves and shrines. Deobandi institutions, notably a burgeoning archipelago of Deobandi madaris across the Pashtun belt and beyond, received support from the Pakistani government and others to produce mujahideen for Afghanistan both in the Soviet and post-Soviet periods.[8] These Deobandi militant groups also have enjoyed both close connections to and overlapping membership with Deobandi political organizations including personalized factions of the Jamiat Ulema-e-Islam (JUI). Until the February 2008 elections, JUI factions comprised important partners in the Islamist coalition (Muttahida Majlis-e-Amal or MMA) that formed the provincial government in Pakistan's Northwest Frontier Province (NWFP), a coalition government with President Musharraf's political ally (the Pakistan Muslim League-Q) in Balochistan, and the loyal opposition in the national parliament.

A second important school of thought that animates militancy in Pakistan is the Ahl-e-Hadith interpretative tradition. The most prominent Ahl-e-Hadith militant group is the Lashkar-e-Taiba (LeT). Ahl-e-Hadith is a Sunni interpretative tradition associated with Hanbali school of jurisprudence, which in Pakistan is sometimes called Salafist or derogatorily "Wahabbist." The Ahl-e-Hadith tradition is the South Asian variant of the theological tradition motivating core al Qaeda ideologues. While LeT is most known for its militant activities, one of the organization's crucial functions is the expansion of the market share of Ahl-e-Hadith adherents in Pakistan. For this reason, LeT trains many more potential militants than it will ever deploy for operations. LeT expects these recruits to return to their localities and continue propounding support for LeT and its creed.[9]

Several groups operating in Kashmir (e.g. Hizbul Mujahideen and related factions such as Al Badr) are associated with Jamaat-e-Islami (JI), which is a supra-sectarian school of thought and Islamist political party in Pakistan. Jamaat-e-Islami, while formally a political party, espouses the ideological leanings of its founder Maulana Maududi. Jamaat-e-Islami is similar in goals and outlook to the Muslim Brotherhood. JI was, until the 2008 elections, a member of the Islamist bloc (the MMA) despite growing differences between JI and the Musharraf government and with other Islamist leaders within the MMA who continued to support Musharraf. JI boycotted the 2008 elections.

In addition to these schisms across interpretative traditions, Pakistan's militant groups can in some measure be distinguished by their historical and current goals. As will be discussed herein some of these goals have changed or have not always been stable. For example, groups such as Jaish-e-Mohammad (JM), Lashkar-e-Taiba (LeT) and Hizbul Mujahideen (HM) have traditionally focused upon the Kashmir issue. Only the HM and other JI-related groups have limited their operations to Indian-administered Kashmir.[10] From 1999 if not earlier, LeT and JM began operations in the Indian hinterland both in the name of "liberating Kashmir" but also in the name of a wider jihad in India and exacerbating Hindu-Muslim discord with-

---

into Chaos: The U.S. and the Disaster in Pakistan, Afghanistan, and Central Asia (New York: Penguin, 2009); See Husain Haqqani, *Pakistan Between and Military* (Washington, DC: CEIP, 2005); Hassan Abbas and Jessica Stern, *Pakistan's Drift Into Extremism: Allah, then Army, and America's War Terror* (New York: M.E. Sharpe 2004).

[7] This draws from C. Christine Fair, "Who Are Pakistan's Militants and Their Families?" *Terrorism and Political Violence,* Vol. 20, No. 1 (January, 2008).

[8] Steve Coll, *Ghost Wars: The Secret History of the CIA, Afghanistan, and Bin Laden, from the Soviet Invasion to September 10, 2001* (New York: Penguin, 2004). Pakistan developed and supported Islamist proxies in Afghanistan before the Soviet invasion by mobilizing those Islamists who had been ousted by President Daud after 1973.

[9] See C. Christine Fair, "Militant Recruitment in Pakistan: Implications for Al-Qa'ida and Other Organizations," *Studies in Conflict and Terrorism,* Vol. 27, No. 6 (November/December 2004).

[10] There have been some reports that these groups are operating in Afghanistan. I have been unable to confirm these reports.

in India to undermine India's claims to be a diverse democracy that accommodates the aspirations of its varied religious and ethnic groups.[11]

In addition, Pakistan hosts a number of sectarian groups such as the Deobandi Lashkar-e-Jhangvi (LeJ) and Sipah-e-Sahaba-e-Pakistan (SSP) which traditionally focused upon anti-Shia targets. These groups have also had a historical presence in Afghanistan as well. In the past, Iranian-backed Shia militias such as the Tehreek-e-Jafria and the Sipah-e-Muhammad have targeted Sunnis, especially those propounding an explicit anti-Shia agenda. These groups were particularly active throughout the 1990's. While the Deobandi-Shia axis garners the most attention with respect to sectarian violence, it should be noted that considerable violence and discord exists among Pakistan's various Sunni traditions (maslaks).

From as early as 2002, some elements of Pakistan's varied Deobandi groups (e.g. JM, HUJI, LeJ, SSP) began targeting the Pakistan state as evidenced by the attacks on then President Musharraf, various civilian leaders including the Ministry of Interior and former Prime Minister Benazir Bhutto, and numerous military, police and intelligence individuals and organizations. Analysts believe that these groups disagreed with President Musharraf's policies of supporting the United States and its military campaign in Afghanistan as well as Musharraf's policy of "moderated jihad" in Kashmir. Musharraf adopted this approach due to, inter alia, increased international pressure in the wake of the Indian Parliament attack in December 2001 by Pakistan-based militants. That attack triggered the largest amassing of Indian and Pakistani troops and stoked international fears of an Indo-Pakistan war. Indian diplomatic fortitude was again tested when the LeT massacred wives and children of army personnel in Kaluchak. The United States engaged in vigorous diplomacy to dampen the compound crisis and avert conflict. In response to the Indian mobilization, Pakistani troops swung from the west to the east which compromised U.S. operations in Afghanistan.

Pakistan's various Deobandi groups have also been responsible for numerous attacks against international targets such as the various attacks on the U.S. Consulate in Karachi, the suicide attack against numerous French naval engineers working in Karachi, a church in Islamabad frequented by foreigners, among numerous others.[12] Notable among these groups attacking Pakistani and international targets within Pakistan are JM, HUJI, and LeJ/SSP.

Following Pakistan's military operations in the Pashtun belt and U.S. military operations in Afghanistan, a series of Pashtun-led militant commanders emerged that began targeting the Pakistani security forces including the regular army, paramilitary organizations such as the Frontier Corps and police. In late 2007, many of these commanders coalesced under the banner of the "Pakistani Taliban" (e.g. Tehreek-e-Taliban-e-Pakistan) under the leadership of Baitullah Mehsood based in South Waziristan in Pakistan's federally Administered Tribal Areas (FATA). Mehsood claims many allies all of whom to seek to establish in various degrees sharia (Islamic governance) across the Pashtun belt in Pakistan including the FATA and settled areas such as Swat.[13] In late February 2008, two dissident commanders (Mullah Nazir of South Waziristan and Gul Bahadur of North Waziristan) set aside their differences with Baitullah Mehsood and forged the Shura Ittehad-ul-Mujahiden.[14]

In addition to the above noted Pakistani groups, Pakistan also hosts elements of the Afghan Taliban, with leadership committees (shuras) in Quetta, Peshawar, and

---

[11] In 1999, the LeT attacked an intelligence outpost attached to the Red Fort, a high profile tourist destination in New Delhi. In 2001, Jaish-e-Mohammad attacked India's parliament building.

[12] For an inventory of post-9/11 "western" attacks in Pakistan, see South Asia Terrorism Portal, "Post-9/11 Attacks on Western Targets in Pakistan," no date. Available at *http://www.satp.org/satporgtp/countries/pakistan/database/westerntargets.htm.*

[13] See Hassan Abbas, "Increasing Talibanization in Pakistan's Seven Tribal Agencies," *Terrorism Monitor* Vol. 5, No. 18 (September 27, 2007), pp. 1–5; Hassan Abbas, "A Profile of Tehrik-i-Taliban Pakistan" *CTC Sentinel,* Vol. 1, No. 2, January 2008, pp. 1–4; Syed Shoaib Hasan, *"Profile: Baitullah Mehsud,"* BBC News, December 28, 2007. Available at *http://news.bbc.co.uk/2/hi/south_asia/7163626.stm.*

[14] Pakistan has considered Maulvi Nazir an ally because he helped oust or kill numerous Uzbeks in South Waziristan. He is considered to be a dedicated foe of U.S. and NATO forces as he dispatches fighters to Afghanistan. Gul Bahadar has had a number of differences with Baitullah Mehsood. It is not clear what this alliance means for Pakistan or for the United States and allies in Afghanistan. See Saeed Shah, "Taliban rivals unite to fight US troop surge," *The Guardian,* March 3, 2009. Available at *http://www.guardian.co.uk/world/2009/mar/03/taliban-pakistan-afghanistan-us-surge.*

Karachi.[15] The Afghan Taliban remains focused upon ousting foreign forces in Afghanistan, overthrowing the Karzai regime, and restoring their role in governing Afghanistan. As is well known, Pakistani territory is also used by al Qaeda. Al Qaeda operatives are known to reside in North and South Waziristan and Bajaur among other areas in the Pashtun belt. Moreover, many al Qaeda operatives (such as Abu Zubaidah, Khalid Sheikh Mohammad among numerous others) have been arrested in Pakistani cities.[16]

Pakistan has rightly noted that it is a victim of sanguinary terrorist violence that has escalated since joining the U.S.-led war on terror. Indeed, the TTP and other sectarian and ethno-nationalist militants in Pakistan have wreaked considerable havoc in Pakistan with 63 suicide attacks and an astonishing 2,148 attacks or clashes with security forces in 2008 alone.[17]

Howsoever horrific these facts are, the LeT has never targeted the Pakistani state or international targets within Pakistan. This has led many analysts within and without the region to intuit that LeT continues to enjoy special relations with Pakistan's intelligence and military agencies notwithstanding much-touted Pakistani efforts to proscribe LeT's activities and those of its cover organization, the Jamaat ul Dawa (JuD). The March 2, 2009 attack on the Sri Lankan cricket team in Lahore may signal an important shift in LeT operations and its ties to the state. In that incident, several heavily armed men viciously assaulted the team, umpires, and related officials as well as their police escort in the Punjabi city of Lahore, killing six police officers and two civilians. Speculation is rife that the commando operation may have been the handiwork of the LeT. If so, this attack will be the first LeT attack on Pakistani soil. At the time of writing, it is too early to inveigh upon the evidence for or against these allegations of LeT involvement.

While the verdict is out on perpetrators of the attack on the Sri Lankan cricketers, few analysts and journalists interviewed during my recent trip to Pakistan believed that Pakistan could or would decisively eliminate JuD despite its late 2008 ban on the organization. This is both because JuD/LeT is still considered to be an important asset in Pakistan's quest to secure its regional objectives and because it, unlike the proliferating morass of Deobandi groups, has never targeted the state. However, even if Pakistan were to resolve to eliminate JuD/LeT, few believe that Pakistan has the ability to do so.

LASHKAR-E-TAIBA: ORIGINS, OPERATIVES, AND OPERATIONS

The LeT has focused the attention of policymakers in recent months because it perpetrated the November 2008 terrorist attacks in Mumbai. As this section narrates, the LeT has a long-standing presence in Pakistan and South Asia. Since 2001, it has increasingly established a presence well beyond the region. LeT emerged as the military wing of the Markaz Daawat ul Irshad (MDI), headquartered in Muridke near the Punjabi city of Lahore. MDI was founded in 1986 by two Pakistani Engineering professors, Hafiz Muhammad Saeed and Zafar Iqbal. Abdullah Azzam, a close of associate of Bin Laden who was affiliated with the Islamic University of Islamabad and the Maktab ul Khadamat (Bureau of Services for Arab mujahideen), also provided assistance. He was killed in Peshawar 2 years after the Markaz was founded. MDI, along with numerous other militant groups, was involved in Afghanistan from 1986 onwards and established militant training camps for this purpose. One camp was known as Muaskar-e-Taiba in Paktia (in Afghanistan bordering Pakistan) and a second known as Muaskar-e-Aqsa in the Kunar province of Afghanistan.[18] (Kunar is known to be home to numerous Ahl-e-Hadith adherents in Af-

---

[15] See, inter alia, Senator Carl Levin, "Opening Statement of Senator Carl Levin, Senate Armed Services Committee Hearing on Afghanistan and Pakistan," February 26, 2009. Available at *http://levin.senate.gov/newsroom/release.cfm?id=308740*; Ian Katz, "Gates Says Militant Sanctuaries Pose Biggest Afghanistan Threat," *Bloomberg News,* March 1, 2009. Available at *http://www.bloomberg.com/apps/news?pid=20601087&sid=aehmlRXgKi2o&refer=home*; Barnett R. Rubin. "Saving Afghanistan," *Foreign Affairs,* January/February 2007. Available at *http://www.foreignaffairs.org/20070101faessay86105-p0/barnett-r-rubin/saving-afghanistan.html*;[sic]

[16] See comments made by National Intelligence Director John Negroponte cited in "Al-Qaeda 'rebuilding' in Pakistan," *BBC News Online,* January 12, 2007. Available at *http://news.bbc.co.uk/2/hi/south_asia/6254375.stm;* K. Alan Kronstadt, *U.S.-Pakistan Relations* (Washington, DC: Congressional Research Service, 2008). Available at *http://fpc.state.gov/documents/organization/115888.pdf.*

[17] See Pak Institute for Peace Studies, *Pakistan Security Report 2008* (Islamabad: PIPS, 2009) p. 3.

[18] See Yoginder Sikand, "The Islamist Militancy in Kashmir: The Case of the Lashkar-e-Taiba," in Aparna Rao et al. Eds. *The Practice of War: Production, Reproduction and Communication of Armed Violence* (New York: Berghahn Books, 2007), pp. 215–238; Mariam Abou

ghanistan, which overall has few followers in that country. For this reason, Kunar has been an attractive safe-haven for Arabs in Afghanistan.) Pakistan-based analysts note that MDI/LeT's training camps were always separate from those of the Taliban, which hosted Deobandi militant groups such as HUJI and Harkat ul Mujahideen. This has led some analysts to contend that LeT has not had the sustained and organic connections to al Qaeda as enjoyed by the Deobandi groups, many of which became "out sourcers" for al Qaeda in Pakistan.[19]

In 1993, MDI divided its activities into two related but separate organizations: MDI continued the mission of proselytization and education while LeT emerged as the militant wing. The ISI is believed to have funded the organization and analysts continue to believe that LeT is a close proxy of Pakistani intelligence agencies.[20] After the Soviets withdrew from Afghanistan, LeT/MDI shifted focus to Indian-administered Kashmir. It staged its first attack (against a jeep carrying Indian air force personnel) in Kashmir in 1990. The vast majority of LeT operatives are Pakistanis (often Punjabis) and the organization has spawned a vast training infrastructure throughout the country to support its dual mission of training militants and converting Pakistanis to the Ahl-e-Hadith interpretative tradition. For much of the 1990's (with few exceptions), LeT operations were restricted to Indian administered Kashmir.

A perusal of LeT literature demonstrates a commitment to targeting Indian Hindus, Jews, Americans and other infidels and apostate Muslims; stoking larger Hindu-Muslim discord in India; and liberating all of India and establishing a caliphate.[21] MDI claims that it has had a leading role in armed struggles across the Muslim world, first in Afghanistan, then in Bosnia, Chechnya, Kosovo, the Philippines, and Kashmir among other venues.[22] While there is no independent verification of these claims, as discussed herein, many LeT-associated individuals and cells have appeared in Iraq, Australia, the United States, the United Kingdom and several European countries.

LeT has a hallmark modus operandi which has often been misconstrued as "suicide operations." In fact, LeT does not do suicide operations per se in which the goal of the attacker is to die in the execution of the attack. Rather, LeT's "fidayeen" missions are more akin to high-risk missions in which well-trained commandos engage in fierce combat during which dying is preferable to being captured. While martyrdom is in some sense the ultimate objective of LeT operatives, the LeT selects missions where there is a possibility (howsoever slim) of living to kill more of the enemy. The goal of LeT commandos therefore is not to commit suicide in the execution of an attack. Rather, they seek to kill as many as possible until they either succumb to enemy operations or manage to survive, perhaps by decisively eliminating the enemy in the battle.

Zahab has described a typical LeT encounter in the following way "the fighters are well trained and highly motivated and they engage the enemy on its own terri-

---

Zahab, "I Shall be Waiting at the Door of Paradise: The Pakistani Martyrs of the Lashkar-e-Taiba (Army of the Pure)", in Aparna Rao et al. Eds. *The Practice of War: Production, Reproduction and Communication of Armed Violence* (New York: Berghahn Books, 2007), pp.133158 [sic]; Saeed Shafqat, "From Official Islam to Islamism: The Rise of Dawat-ul-Irshad and Lashkar-e-Taiba," in Christophe Jaffrelot Ed. *Pakistan: Nationalism without a Nation* (London: Zed Books, 2002), pp. 131–147.

[19] In 1998, the United States bombed several al Qaeda/Taliban training camps in retaliation for the al Qaeda attacks on U.S. embassies in Africa. Militants of several Pakistani Deobandi groups were killed including operatives of HUJI and HuM among others. See Barry Bearak, "After The Attacks: In Pakistan; Estimates Of Toll In Afghan Missile Strike Reach As High As 50," *The New York Times,* August 23, 1998. Also see Dexter Filkins, "'All of Us Were Innocent,' Says Survivor of U.S. Attack on Camp," *The Los Angeles Times,* August 24, 1998. Available at *http://articles.latimes.com/1998/aug/24/news/mn-16045.*

[20] Analysts believe that the LeT, with its explicit Islamist and pro-Pakistan orientation, was established to counter the ethno-nationalist and pro-independence militant group Jammu Kashmir Liberation Front (JKLF). The JKLF eventually abandoned militancy and assumed political activism. For more information about LeT's origins, see Yoginder Sikand, "The Islamist Militancy in Kashmir: The Case of the Lashkar-e-Taiba," in Aparna Rao et al. Eds. *The Practice of War: Production, Reproduction and Communication of Armed Violence* (New York: Berghahn Books, 2007), pp. 215–238; Mariam Abou Zahab, "I Shall be Waiting at the Door of Paradise: The Pakistani Martyrs of the Lashkar-e-Taiba (Army of the Pure)", in Aparna Rao et al. Eds. *The Practice of War: Production, Reproduction and Communication of Armed Violence* (New York: Berghahn Books, 2007), pp.133158[sic]; Saeed Shafqat, "From Official Islam to Islamism: The Rise of Dawat-ul-Irshad and Lashkar-e-Taiba," in Christophe Jaffrelot Ed. *Pakistan: Nationalism without a Nation* (London: Zed Books, 2002), pp. 131–147.

[21] The author has collected LeT poster work and written materials since 1995.

[22] Sikand, "Islamist Militancy in Kashmir," P. 219. Also see discussion of LeT in Muhammad Amir Ranan (trans. Saba Ansari) *The A to Z of Jehadi Organizations in Pakistan* (Lahore: Mashal, 2004), pp. 324.

tory. Small groups of fedayeen . . . storm a security force camp and kill as many soldiers as possible before taking defensive positions within the camp and engaging security force personnel till they attain martyrdom. Battles often last twenty hours, if not more."[23] She further notes that these spectacular and well-planned attacks bring the LeT maximum publicity, expands recruiting and donations and demoralizes the enemy which must resort to heavy fire, which destroys their own buildings and causes substantial collateral damage in the process. While LeT claims that it has only assaulted hard targets, their record demonstrates an absolute willingness to kill civilians in cinemas, hotels, tourist destinations, airports, etc.

Consonant with the rigor of a typical LeT mission, LeT recruits do not predominantly draw from Pakistan's madaris (pl. madrassah). Rather LeT recruits are generally in their late teens or early twenties and they tend to be better educated than Pakistanis on average or even other militant groups such as the Deobandi SSP or JM. A majority of LeT recruits have completed secondary school with good grades and some have even attended college. This reflects both the background of LeT's founding fathers who were engineering professors and their commitment to technical and other education. Many LeT operatives likely came into contact with LeT through proselytization programs on college campuses, which in turn lured the potential recruits to the large "ijtema" (congregation) held annually in Muridke. The fraction of madrassah-educated LeT operatives is believed to be as low as 10 percent.[24] Clearly not all LeT cadres are well-educated as attested by the lone surviving Mumbai gunman, Azam Amir Kasab, a Punjabi with only a fourth-grade education. By comparison, the mean years of schooling for males in the Punjab is 4.7 years.[25] LeT also actively targets women both to expand their recruitment base of males and reportedly to recruit women for militant operations.[26] In sharp contrast, many of the Deobandi groups including the Afghan Taliban rely upon madrassah and mosque-based networks.[27]

Since the late 1990's, LeT has cultivated significant operational reach beyond Kashmir and into India. While Indian citizens were always required for facilitating LeT and other militant groups' actions within Indian-administered Kashmir and the Indian hinterland, LeT has successfully cultivated active cadres and figures preeminently in founding of the Indian Mujahideen. In 2002, at least 14 young men from Hyderabad left for Pakistan for training, reportedly motivated by the massacre of Muslims in Gujarat in 2002. (Praveen Swami reports that even as early as 1992 some Indian Muslims sought training in Pakistan in response to the demolition of the Babri Masjid by Hindu extremists.) The Hyderabad operatives received training in LeT and JM camps and enjoyed operational assistance from Bangladesh-based Harkat-ul-Jihad-Bangladesh (HUJI–B). This cell was responsible for the May 18, 2007 terrorist attack in Hyderabad's Toli Chowki area.[28] LeT has moved Indian personnel into and out of Pakistan via Bangladesh and other countries through criminal syndicates as well as other Islamist and militant groups such as the Students Islamist Movement of India (SIMI) and Harkat-ul-Jihad-Bangladesh (HUJI–B) among others.[29]

Despite the rhetoric surrounding the horrific events in Mumbai on November 26, 2008, there were important antecedents of that attack. Most recently, in July 2006, LeT working with local operatives, detonated seven explosions across Mumbai's commuter rail system. That 2006 assault was even more lethal than the 2008 carnage, killing at least 187. While that attack focused the public's attention upon LeT's ability to strike deep within India, LeT had reportedly established networks in Mumbai as early as August 1999. India's intelligence bureau disrupted a pan-India network led by LeT-operative Amir Khan who was tasked with recruiting from India's communal-violence afflicted communities. In 2000, Indian authorities intercepted three

---

[23] Zahab, "I Shall be Waiting," p. 138.

[24] Zahab, "I Shall be Waiting," p. 140, Shafqat, "From Official Islam to Islamism," p. 142.

[25] Data on mean years of schooling is given for 2005. See Social Policy Development Center. *Social Development in Pakistan: Annual Review* (Karachi: SPDC, 2007), p. 152. Available at *http://www.spdcpak. com/pubs/sdip0607.pdf.*

[26] Farhat Haq, "Militarism and Motherhood: The Women of the Lashkar-i-Tayyabia in Pakistan," *Signs,* vol. 32, no. 4, Summer 2007, pp. 1023–1046.

[27] For a more throughout discussion of the connections between militancy and education, see C. Christine Fair, *The Madrassah Challenge: Militancy and Religious Education in Pakistan* (Washington, DC: USIP, 2008).

[28] Praveen Swami, "Terror Junction," *Frontline,* Vol. 24, No. 11, June 2–15, 2007. Available at *http://www.hindu.com/fline/fl2411/stories/20070615002303500.htm.*

[29] Praveen Swami, "Lashkar-trained Indian Terrorists Pose Growing Threat," *The Hindu,* December 19, 2008. Available at *http://www.hindu.com/2008/12/19/stories/2008121956141200.htm.*

Pakistani LeT cadres who had planned to kill Bal Thackeray, leader of a Hindu nationalist group called the Shiv Sena.[30]

In 2004, another LeT cell was disrupted that aimed to attack the Bombay Stock Exchange. (The Bombay Stock Exchange had been attacked previously in 1993. The then India-based Mafioso, Dawood Ibrahim, orchestrated that attack using Indian militants with Pakistani support.) In June 2006, the Maharashtra police arrested an 11-member LeT cell that shipped some 43 kilograms of explosives, assault rifles and grenades to India using sea routes. Several of those militants had ties to SIMI. Indian analysts believe that LeT, working with SIMI and smuggling rings, have been able to successively move large amounts of explosives and weapons by sea along the Gujarat coast.[31] The movement of explosives through the Maharashtra and Gujarat coastlines was reminiscent of logistical routes used to supply explosives for the 1993 Bombay Stock Exchange.[32]

Needless to say, these are only illustrative—not exhaustive—examples of LeT's penetration of India and cultivation of Indian networks to conduct terror operations. With respect to the November 2008 attack, at least two Indian operatives played critical roles: Fahim Arshad Ansari, a key LeT operative from Mumbai, and Sabahuddin Ahmad of Uttar Pradesh. Both men helped prepare maps and videotapes to guide LeT's operatives to their targets. Their contributions—perhaps more so than the use of GPS devices—likely guided the terrorists' movements through Mumbai.[33]

Finally, the early connections between MDI/LeT to Azam, along with the organization's Salafijihadi outlook, fosters suspicion that LeT and al Qaeda enjoy tight linkages. These suspicions are buttressed by a number of developments and observations. First, al Qaeda operatives (e.g. Abu Zubaidah) have been arrested in LeT safe houses. In addition, LeT has been operating against U.S., NATO and Afghan forces in Kunar and Nuristan in close proximity to al Qaeda, which operates in the same region.[34] Third, in recent years, LeT operatives have appeared in small numbers in other theatres. For example, British forces captured two Pakistani LeT operatives in Iraq and rendered them into U.S. custody.[35] A number of Australians (including apparent converts to Islam) have been trained in LeT camps and have plotted to attack Australian targets, discomfiting Australian authorities.[36] Reports persist that a wide array of American, Canadian, and British nationals have trained in LeT camps.[37] At least one of the bombers (Shahzad Tanveer) in London's "7/7" subway attack is alleged to have contacted LeT officials while in Pakistan as well as those associated with JM. Apart from that incident, British officials contend that LeT has numerous links with many terror cells and plots disrupted in the United Kingdom. For example, Dhiren Barot, a Hindu convert to Islam and LeT activist was arrested

---

[30] Praveen Swami, "Road to Unimaginable Horror," *The Hindu,* July 13, 2006. Available at *http://www.hindu.com/2006/07/13/stories/2006071303420800.htm.*

[31] In May 2006, Mohammad Iqbal, an LeT activist from Bahawlpur (a city in southern Punjab in Pakistan), was shot dead by Delhi Police. Iqbal had worked through mafia-linked traffickers to ship a consignment of explosives through Gujarat that was used in the February 2006 attack on an Ahmedebad (Gujarat) train platform, See Praveen Swami, "Road to Unimaginable Horror," *The Hindu,* July 13, 2006. Available at *http://www.hindu.com/2006/07/13/stories/2006071303420800.htm.*

[32] See Praveen Swami and Anupama Katakam, "Investigators Shut Down Terror Cells Tasked with Executing Strikes in Gujarat, but the Threat Remains," *Frontline,* Vol. 23, No. 10, May 20–June 2, 2006.

[33] Y.P. Rajesh and Sagnik Chowdhury, "26/11 The Indian hand," Indian Express, February 27, 2009. Available at *http://www.indianexpress.com/news/26-11-the-indian-hand/428565/.*

[34] Author fieldwork in Afghanistan between June and October 2007; Kathy Gannon, "Pakistan militants focus on Afghanistan: Jihadist groups are increasingly attacking U.S., NATO forces in Afghanistan," Associated Press, Web site, July 14, 2008.

[35] Richard Norton-Taylor, "Britain aided Iraq terror renditions, government admits," *The Guardian,* February 26, 2009. Available at *http://www.guardian.co.uk/world/2009/feb/26/britain-admits-terror-renditions.*

[36] Recently, during a trial of several men plotting to attack the United States from Sydney, a participant (a Korean-American Muslim convert) alleged that an Australian citizen known as Abu Asad trained with Lashkar-e-Taiba at a camp in Pakistan in 2001. See Geesche Jacobsen, "Australian in training camp named," *Sydney Morning Herald,* January 13, 2009. Available at *http://www.smh.com.au/news/national/australian-in-training-camp-named/2009/01/13/1231608682540.html.* For information on another collective of Australians trained in LeT camps, see Ashok Malik, "Lashkar link in Aussie terror net," *Indian Express,* June 12, 2004. Available at *http://www.indianexpress.com/oldstory.php?storyid=48832.* Perhaps the most famous Australian to train at an LeT camp is David Hicks who was recently freed from Guantanamo. See "David Hicks: 'Australian Taleban,'" *BBC News*, May 20, 2007. Available at *http://news.bbc.co.uk/2/hi/asia-pacific/3044386.stm.*

[37] See for example "Lashkar training in US, Canada, UK, Australia," *Rediff.com,* December 10, 2008. Available at *http://www.rediff.com/news/2008/dec/10mumterror-lashkar-training-in-us-canada-ukaustralia.htm.*

in the United Kingdom and charged with planning several chemical and radiological attacks on financial offices in the United States. LeT is also tied to Richard Reid (a.k.a. "the shoe bomber") as well as a Virginia-based "paintball jihad" cell in which several Islamists, including an American Muslim convert named Randall "Ismail" Royer, trained to participate in LeT's campaign against India. Royer, who was convicted, dispatched recruits to an LeT camp in Pakistan where they learned to use small arms, rocket-propelled grenades, among other military resources to fight in India.[38]

Pakistan-based analysts of LeT, among others, tend to discount the claims of explicit al Qaeda-LeT linkages and note that al Qaeda operatives have been arrested in Jamaat Islami safe houses as well and note that LeT infrastructure in Afghanistan, as described above, was separate from that of Al Qaeda and their patrons, the Taliban.[39] Thus the actual degree to which LeT is allied to al Qaeda remains an important empirical question. However, LeT threatens U.S. interests irrespective of its formal ties—or lack thereof—to al Qaeda. LeT has well-established linkages to international terrorism and it espouses goals that are similar to those of al Qaeda as the foregoing discussion illustrates.

IMPLICATIONS OF THE NOVEMBER 2008 MUMBAI ATTACK: ANTECEDENTS AND INNOVATIONS

The November 2008 attack bears many hallmarks of previous LeT attacks. The assault employed dedicated and well-trained commandos who used explosives, small arms and grenades—all but one of whom fought until their deaths. While the available evidence suggests that the main operators were Pakistani, the attack relied upon crucial domestic assistance. Like previous LeT attacks in Mumbai and elsewhere, this assault involved exclusively soft targets with little or no defenses. Several of the targets (such as the Taj and Oberoi hotels) were Indian icons and reflected the opulence of India's elite. They also attracted wealthy international visitors. Other targets such as the Chatrapati Shivaji Station rendered India's middle and lower-middle classes vulnerable. (The train station was previously known as Victoria Terminus and was renamed after an important 17th century Hindu leader who re-established Hindu political dominance in the region after a long period of Muslim rule.) Other targets, such as the Chabad House, reflect an explicit expansion of LeT's focus as described below.

Most accounts of the attack dilate upon the daring infiltration of the attackers who traveled from Pakistan by sea. While the sea-based landing of the ten militants was exceptionally daunting, the concept was not entirely new even if the complexity of the movement was. As noted, mafia syndicates and Islamist militant groups have moved explosives, guns, grenades and other illicit cargo through similar routes since at least 1993. In the conduct of the 1993 Bombay Stock Exchange, mafia leader Dawood Ibrahim working with an associate named Tiger Memon, arranged for considerable illicit cargo to move into a small fishing village near Mumbai via a small motorboat. In one of the few comprehensive accounts of that conspiracy, S. Hussain Zaidi describes how Memon and his crew boarded a small motorboat which "sailed toward the open sea" where it "rendezvoused [sic] with a large red speedboat," from which it loaded the weapons and other materials (including AK–47s, large quantities of a military grade explosive called RDX, pencil detonators, grenades, pistols) used for the attack. They then returned to the fishing village and offloaded the cargo. While the operatives of the 1993 blast exploited the widespread belief that that Mumbai security forces were inept, the locally recruited participants were ill-prepared for the operation and unfamiliar with the weapons to be used. Dawood Ibrahim and Tiger Memon arranged for their transportation to and from Pakistan where they were reportedly trained by Pakistani intelligence.[40]

---

[38] For more details about the "paintball jihad" cell, see Stephen Schwartz, "Lashkar-e-Taiba in America: A convicted terror recruiter plays victim of the NSA," *The Weekly Standard,* December 16, 2006. *http://www.weeklystandard.com/Content/Public/Articles/000/000/015/927uxqry.asp.*

[39] See Yoginder Sikand, "The Islamist Militancy in Kashmir: The Case of the Lashkar-e-Taiba," in Aparna Rao et al. Eds. *The Practice of War: Production, Reproduction and Communication of Armed Violence* (New York: Berghahn Books, 2007), pp. 215–238; Saeed Shafqat, "From Official Islam to Islamism: The Rise of Dawat-ul-Irshad and Lashkar-e-Taiba," in Christophe Jaffrelot Ed. *Pakistan: Nationalism without a Nation* (London: Zed Books, 2002), pp. 131–147. Why their infrastructure was apart from the other Deobandi camps is an important question even if there are no solid answers. Two possible explanations include: (1) Be deliberate ISI decision to keep MDI/LeT separate from other groups' camps or, (2) more likely, the deep-seated hostility that MDI/LeT has historically had toward Deobandis and vice versa.

[40] S. Hussain Zaidi, *Black Friday: The True Story of the Bombay Bomb Blasts* (New Delhi: Penguin, 2002), pp. 50–67.

However, other aspects of this attack were notable and distinctive. While LeT has been operating against U.S., NATO, and Afghan forces in Kunar and Nuristan[41] and while LeT operatives went to fight allied forces in Iraq, this was the first known LeT assault upon American and international civilians. While it is now believed that LeT did not single out foreigners across the targets, one target in particular was distinctive: the Chabad Center. Mumbai, among other cities, hosts a historical albeit shrinking Jewish population and boasts many historical synagogues and Jewish cultural facilities. Despite the decades of Islamist violence perpetrated by a range of groups espousing an anti-Semitic agenda, no Islamist militant group had ever targeted India's Jewish community. Chabad was distinctive because it was not merely Jewish, but also associated with Israelis and other international Jewish visitors.[42] This target is most curious of all as few from or familiar with Mumbai have ever heard of this institution.[43]

While LeT and other groups have often posited and resisted the "Brahmanic-Talmudic-Crusader" alliance, no militant group within South Asia violently operationalized this agenda until the Mumbai 2008 attack. In the case of LeT, it is puzzling that despite advocating this agenda since the late 1980's, it took nearly two decades to act upon it. Possible explanations for the choice of that target include the growing Indo-Israeli military, counterterrorism, and intelligence relationship which has long irritated Pakistan and animated the rhetoric of Islamist militants across the region.[44] Moreover, Israeli lobby apparatus in the United States has nurtured India's own emergent lobbying organizations and is rightly or wrongly associated with helping India achieve the Indo-U.S. nuclear deal.[45] Thus the selection of the Chabad center—rather than any of India's domestic Jewish institutions—may have sought to undermine this important bilateral relationship. Transcripts of the phone intercepts of the attack at the Chabad house buttress this explanation. The Pakistan-based caller encouraged the attacker to kill the hostages arguing that "If the hostages are killed, it will spoil relations between India and Israel."[46] Another explanation may be that LeT was emboldened by its attacks against U.S. forces in Afghanistan and influenced by al Qaeda co-located with LeT in Afghanistan's Kunar and Nuristan provinces. Of course, both may be valid.

CONCLUSIONS: IMPLICATIONS FOR U.S. REGIONAL, AND INTERNATIONAL SECURITY

U.S. policymakers and analysts have pondered whether LeT could or would undertake such operations within the United States. As the foregoing suggests, a number of individuals (including converts) who appear to have radicalized in the diaspora have traveled to Pakistan to train with the LeT and other militant groups (e.g. JM). LeT and other militant groups in the Punjab, comprise an important link between those who have radicalized in the diaspora and Pakistan's tribal areas where al Qaeda is ensconced. (In turn Pashtun militants from the tribal areas rely upon Pashtun networks as well as Punjabi networks to execute attacks throughout Paki-

---

[41] Author fieldwork in Afghanistan between June and October 2007; Kathy Gannon, "Pakistan militants focus on Afghanistan: Jihadist groups are increasingly attacking U.S., NATO forces in Afghanistan," Associated Press, Web site, July 14, 2008.

[42] Yair Ettinger, "Mumbai attack sends shock waves through Chabad community worldwide," *Haaretz,* November 29, 2008. Available at *http://www.haaretz.com/hasen/spages/1041785.html*; Anshel Pfeffer, "9 dead in Mumbai Chabad house attack; Israel to help identify bodies," *Haaretz,* November 30, 2008. Available at *http://www.haaretz.com/hasen/spages/1041834.html.*

[43] Conversations with Indian journalists and others during a recent trip to India and based upon conversations with a relative who lives in Mumbai.

[44] Military and intelligence ties have in many ways formed the backbone of the Indo-Israeli relationship and Israel is now India's pre-eminent arms supplier. For an early account of the emerging relationship see P.R. Kumaraswamy, "Strategic Partnership Between Israel and India," *MERIA Journal,* Vol. 2, No. 2, May 1998. Available at *http://meria.idc.ac.il/journal/1998/issue2/jv2n2a6.html.* See Embassy of Israel, New Delhi, "Indo-Israel Relations," n.d. Available at *http://delhi.mfa.gov.il/mfm/web/main/document.asp?SubjectID=2010&MissionID=93&LanguageID=0&StatusID=0&DocumentID=-1*; P R Kumaraswamy, "Indo-Israeli military ties enter next stage: A US$2.5 billion Indo-Israeli defense project marks a new phase in the two countries' relations," ISN, August 3, 2007. Available at *http://www.isn.ethz.ch/isn/Current-Affairs/Security-Watch/Detail/?ots591=4888CAA0-B3DB-1461-98B9-E20E7B9C13D4&lng=en&id=53611*; Efraim Inbar, "The Indian-Israeli Entente," *Orbis,* Vol. 48, No. 1, Winter 2004, Pages 89–104.

[45] This judgment is based upon numerous visits to Pakistan since the discussion of the deal emerged.

[46] Andrew Buncombe and Omar Waraich in Islamabad, "Mumbai siege: 'Kill all the hostages—except the two Muslims' Phone conversations between Mumbai attackers and their 'Pakistani handlers' cast chilling new light on massacre," *The Independent,* January 8, 2009. Available at *http://www.independent.co.uk/news/world/asia/mumbai-siege-kill-all-the-hostages-ndash-except-the-twomuslims-1232074.html.*

stan.) During my recent trip to Pakistan, one interlocutor described these Punjab-based groups as the "escalator for foreigners to get to FATA."[47] As FATA remains an important epicenter for international terrorism, the importance of groups like LeT (among others) cannot be understated and should motivate Washington to insist that Pakistan cease all forms of active and passive support for these groups and act decisively to eliminate them.

A smaller number of Pakistani LeT operatives have found their way to other theatres such as Iraq. Given the tenacity of opposition to the U.S. invasion and occupation of Iraq, it is surprising that only two LeT operatives made their way to Iraq suggesting limited capacity or will. Given the difficulty in Pakistan-based operatives to obtain a visa to visit western countries, the strategy of pulling in operatives from the west is likely to be the most productive strategy as these individuals speak English, have the appropriate passport, and are more likely to gain access to targeted countries. Thus even if LeT (and other such groups) may be less capable of dispatching Pakistan-based militants outside of the South Asian theatre, LeT and other militant camps in Pakistan remain destinations for international jihadists who are not so restricted in reaching their desired theatre of operation. Given the terrorist cells that have been disrupted in the United States, United Kingdom, Europe, and Australia (among other venues) and in light of the challenges posed by the visa waiver program, one cannot rule out an LeT-facilitated attack within the United States. After Mumbai, one absolutely cannot rule out further attacks against U.S. citizens or interests abroad or those of U.S. allies.

Even if an LeT attack within the United States may be a low-probability event, LeT poses a number of concerns for the United States not the least of which include on-going operations against U.S. and allied forces in Afghanistan, the likelihood of future attacks in India with the ever-present possibility of prompting yet another Indo-Pakistan military crises, and "copy cat" attacks in the United States or elsewhere.

The challenges faced by the Indian security forces are also illuminating.[48] First, the Indian authorities lacked basic information about the floor plan. Second, the Indian counterterrorism forces were undermined by the media coverage which televised in real time their efforts to eliminate the terrorists. The Pakistan-based handlers, during on-going phone conversations with the militants, relayed critical information gleaned from the coverage, as the intercepted phone conversations attest. Third, given that many of these targets are deeply embedded within organic urban growth, even under the most optimistic assumptions, many of India's numerous high-value civilian (e.g. tourism, commercial, industrial) targets will be difficult to secure.

Finally the Mumbai attack and its sustained media coverage reminds one that militants need not use extravagant suicide bombs to wreak havoc. Rather militants waging coordinated attacks, against several, soft and poorly defended—if not utterly indefensible targets—targets using only small-arms can inflict considerable damage.[49]

Ms. JACKSON LEE. Mr. Bonnell.

STATEMENT OF DAVID BRADLEY BONNELL, DIRECTOR, GLOBAL SECURITY, INTERCONTINENTAL HOTELS GROUP

Mr. BONNELL. Madam Chairwoman, Members of the committee, I want to express my appreciation. It is an honor to speak to you, and I hope that you will find my testimony to be useful. It will certainly be less cerebral than Dr. Fair.

As the terrorist attack on Mumbai unfolded, as it was unfolding, I was in contact with my counterparts with Marriott, Starwood, Hyatt, and Hilton as a direct result of the association that had

[47] Author interviews with Pakistani and foreign journalists, analysts and diplomats in Islamabad in late February 2009.

[48] Some of the challenges faced by the Indian authorities also stemmed from particular enduring lapses in Indian internal security apparatus. These include, among other durable problems, the inability of the National Security Guards to get to Mumbai, police ineptitude, poor means to share intelligence between and across external and domestic intelligence agencies, a deficient system for naval and coastal security. See Angel Rabasa et al. *The Lessons of Mumbai* (Santa Monica: RAND, 2008).

[49] Notably, the Indian government did not limit the televised images of the attack even as Indian commandos began their offensives against the militants.

come to exist as a result of the Department of Homeland Security and the Overseas Security Advisory Council. We were in constant contact throughout the attack sharing information with each other, corroborating fact from fiction, sharing information about resources available to us. We have two managed hotels in Mumbai, two InterContinental hotels. We were able to give them information that was useful.

So, armed with reliable intelligence concerning the nature of the attack as it was occurring, we were able to provide our two properties with useful intelligence that enabled them to increase the level of security in response to this event.

In days following the attack, the Association of Corporate Security Professionals shared information concerning various resources that enabled recovery and the restart of the Mumbai business operations confident that reasonable action had been taken to mitigate what was now a foreseeable and predictable threat in that part of the world.

This association of corporate security professionals evolved as the results of the efforts of the Department of Homeland Security. In bringing private sector security crisis management personnel together in an effort to increase preparedness in the private sector, DHS laid the foundation for an association of hotel corporations that has served my company very well. This relationship between the DHS and the IHG, the InterContinental Hotels Group, has been beneficial about the strategic and tactical level. From enabling corporations to understand what constitutes a viable and defensible disaster recoverable business continuity plan, to how a hotel should effect an evacuation response to a bomb threat, that the Department of Homeland Security has shown us how it can be done.

I would like to refer to Title 9 compliance. Title 9 of the 9/11 Commission Act provided us with a map to crisis management planning expressed in terms of preparedness in the private sector and public sector for rescue, restart, and recovery of operations, they should include a plan for evacuations, adequate communications capabilities, and a plan for continuity of operations.

In seeking to achieve the stated goals of Title 9, Department of Homeland Security enabled private sector security professionals to share best practices through its meetings, conferences, and frequent communications. What has evolved in the hospitality private sector as a result of this information sharing are crisis management counterterrorism programs that are threat-based and intelligence-led.

DHS and the Overseas Security Advisory Council both provide much of the intelligence that is used in deploying resources against emerging threats.

Since the 19th century the legal and moral duty of a hotel concerning safety and security has been articulated in terms of reasonable care, which is legally defined as the manner in which a prudent and responsible person responds to a foreseeable and predictable threat. The threat of a terrorist attack against a hotel has now become a conspicuously foreseeable threat, particularly in those parts of the world where a jihadist threat exists.

There are currently 4,186 hotels around the world bearing the InterContinental hotels groups brands of InterContinental Crowne Plaza Hotels, Indigo Suites, Holiday Inn, Holiday Inn Express, Candlewood Suites and Staybridge Suites. The majority of these hotels are franchised and privately owned.

The world headquarters of my company is located in the United Kingdom near London. The regional office for properties in the Americas is located in Atlanta, Georgia, and the Office for the Asia Pacific region of IHG is located in Singapore.

There are 27 corporate facilities that support the business to include business service center reservation centers, data centers and sales offices.

We seek to fulfill our legal and moral duty concerning safety and security through a crisis management system that has taken a great deal of direction from the goals of Title 9.

Integrated throughout the corporate structure, culture and operation of the InterContinental group is a comprehensive crisis management system that provides a flexible and effective response to foreseeable and predictable threats. The system consists of continuous threat assessment, site-specific emergency action plans and business continuity plans, a senior executive crisis response plan, crisis response teams, an internal communications network and crisis emergency response training program.

The crisis management system responds to a crisis through a process that follows operational management structures, existing lines of communication and established business relationships. By following the organizational chain of command, crisis management escalates as needed through a process that connects all corporate operations to a common crisis command organization.

Our counterterrorism program, as previously stated, is threat-based and intelligence-led. The program consists of categorizing all hotels against a terrorist risk profile, conducting a regional strategic threat assessment from each local hotel, conducting a comprehensive assessment of the capabilities of a hotel to resist an attack, providing a management action plan for increasing security capability, monitoring plan compliance. Our counterterrorism program has been implemented within the context of mandatory compliance with brands standards concerning both operational and structural safety and security.

For example, if a hotel is to be constructed within a region that is categorized as high-risk, security design and engineering requirements are imposed on both corporate and franchise properties. The program is then reinforced through security site visits and quality audits.

It is during the assessment of the property that a determination is made as to plan for evacuation, communication capabilities, and a plan for continuity of operations.

As the counterterrorism evolved, the value of the intelligence and information provided by the U.S. State Department sponsored Overseas Security Advisory Council became apparent. Of equally obvious value was the OSAC-sponsored Hotel Security Group, of which IHG is a member.

We are closely affiliated with the American Society of Industrial Security and NFBA in seeking to acquire knowledge concerning emerging risks and methods of mitigating those risks.

Thank you very much.

Ms. JACKSON LEE. I thank the gentleman for his testimony.

[The statement of Mr. Bonnell follows:]

PREPARED STATEMENT OF DAVID BRADLEY BONNELL

MARCH 11, 2009

SUMMARY STATEMENT

As the terrorist attack unfolded in Mumbai on 23 February, 2009, individuals responsible for the counter terrorism program of their respective corporations were in almost constant contact sharing with each other timely and detailed information concerning the events and circumstances of the attack. From this association of corporate security professionals came a flow of intelligence that facilitated critical crisis response decisionmaking, the effective deployment of resources and the flow of constructive internal communications between global corporate headquarters and hotels impacted by the attack.

Armed with reliable intelligence concerning the nature of the attack as it was occurring, the InterContinental Hotels Group (IHG) was able to provide its two Mumbai properties with instructions and resources that enabled those hotels to quickly secure and defend against an attack.

In days following the attack, this association of corporate security professionals shared information concerning various resources that enabled recovery and restart of Mumbai business operations confident that reasonable action had been taken to mitigate what was now a foreseeable and predictable threat in that part of the world.

This association of corporate security professionals evolved as the result of the efforts of the Department of Homeland Security (DHS). In bringing private sector security and crisis management personnel together in an effort to increase preparedness in the private sector, DHS laid the foundation for an association of hotel corporations that has served IHG well.

The relationship between DHS and IHG has been beneficial at both a strategic and tactical level. From enabling corporations to understand what constitutes a viable and defensible disaster recovery/business continuity plan to how a hotel should effect an evacuation in response to a bomb threat, DHS has shown how it can be done.

TITLE IX COMPLIANCE

Title IX of the 9/11 Commission Act provided us with a map to crisis management planning expressed in terms of,

"Preparedness in the private sector and public sector for rescue, restart and recovery of operations should include (1) a plan for evacuation, (2) adequate communications capabilities, and (3) a plan for continuity of operations."

In seeking to achieve the stated goals of Title IX, DHS enabled private sector security professionals to share best practices through its various meetings, conferences, and frequent communications.

What has evolved in the hospitality private sector as a result of this information sharing are crisis management/counterterrorism programs that are threat-based and intelligence-led. DHS and the Overseas Security Advisory Council (OSAC) both provide much of the intelligence that is used in deploying resources against emerging threats.

LEGAL DUTY

Since the 19th Century, the legal and moral duty of a hotel concerning safety and security has been articulated in terms of "reasonable care" which is legally defined as the, "manner in which a prudent and responsible person responds to a foreseeable and predictable threat." The threat of a terrorist attack against a hotel has now become a conspicuously foreseeable and predictable threat, particularly in those parts of the world where a Jihadist threat exists.

IHG

There are currently 4,186 hotels around the world bearing the InterContinental Hotels Group (IHG) brands of, InterContinental Hotels, Crowne Plaza Hotels, Indigo Suites, Holiday Inn, Holiday Inn Express, Candlewood Suites and Staybridge Suites. The majority of these hotels are franchised and privately owned.

The world headquarters of IHG is located in the United Kingdom near London. The regional office for properties in the Americas is located in Atlanta, Georgia and the office for the Asia Pacific region of IHG is located in Singapore. There are 27 corporate facilities that support the business to include business service centers, reservation centers, data centers, and sales offices.

IHG seeks to fulfill its legal and moral duty concerning safety and security through a crisis management system that has taken a great deal of direction from the goals of Title IX.

IHG CRISIS MANAGEMENT SYSTEM

Integrated throughout the corporate structure, culture and operation of the InterContinental Hotels Group (IHG) is a comprehensive Crisis Management System that provides a flexible and effective response to foreseeable and predictable threats. The system consists of: continuous threat assessment; site-specific emergency action plans and business continuity plans; a senior executive crisis response plan; crisis response teams; an internal communication network; and crisis/emergency response training programs.

The IHG Crisis Management System responds to crisis through a process that follows operational management structures, existing lines of communication and established business relationships. By following the organizational chain of command, crisis management escalates as needed through a process that connects all corporate operations to a common crisis command organization.

The IHG Crisis Management System incorporates for its 27 corporate support facilities viable disaster recovery/business continuity plans and programs. Monitored and tested annually, IHG is confident in its ability to quickly restore essential business functions either from temporary or permanent locations.

Another critical component of the IHG Crisis Management System is the counter terrorism program.

COUNTER TERRORISM PROGRAM

The IHG counter terrorism program is, as previously stated, is threat-based and intelligence-led.

The program consists of:

- Categorizing all IHG hotels against a terrorist risk profile.
- Conducting a regional strategic threat assessment for each hotel location.
- Conducting a comprehensive assessment of the capabilities of the hotel to resist an attack.
- Providing an management action plan for increasing security capability.
- Monitoring plan compliance.

Our counter terrorism program is then implemented within the context of mandatory compliance with brand standards concerning both operational and structural safety and security. For example, if a hotel is to be constructed within a region that is categorized as being high risk, Security Design and Engineering requirements are imposed.

The program is then reinforced through both security site visits and quality audits.

It is during the assessment of the property that a determination is made as to plan for evacuation, communication capabilities and a plan for continuity of operations.

OSAC

As the IHG counter terrorism program evolved, the value of the intelligence and information provided by the U.S. State Department-sponsored Overseas Security Advisory Council (OSAC) became apparent. Of equally obvious value was the OSAC sponsored Hotel Security Group of which IHG is a member.

Like DHS, the OSAC brought private sector security professionals together in an effort to improve the security capability of the business.

IHG is also closely affiliated with the American Society of Industrial Security (ASIS) and NFPA in seeking to acquire knowledge concerning emerging risks and methods of mitigating those risks.

Ms. JACKSON LEE. Mr. Raisch, you are recognized for 5 minutes.

STATEMENT OF WILLIAM G. RAISCH, EXECUTIVE DIRECTOR, NEW YORK UNIVERSITY'S INTERNATIONAL CENTER FOR ENTERPRISE PREPAREDNESS

Mr. RAISCH. Madam Chairwoman, Ranking Member Dent, and distinguished Members of the subcommittee. It is my sincere honor to yet again provide testimony to this committee.

Our primary goal at InterCEP is simple. We have the opportunity to bring together key stakeholders to identify and collaboratively solve problems in the area of emergency preparedness, security, and risk management. It is that problem-solving orientation that I would like to bring to my discussion this afternoon and touch on several key points which are discussed in greater detail in my written remarks, but focus on two particularly foundational opportunities.

The first is that presented in what has been termed Title 9, the Private Sector Preparedness Program called for by Public Law 110–53. This is a program that was championed by this committee and that offers the unique opportunity to begin to establish corporate resilience and preparedness as a core business discipline and connected more clearly with bottom-line benefits than perhaps ever before.

Second, I would like to make a point in the course of my discussion—an appeal, really, for collaborative action to design and build in resilience into the current infrastructure initiatives that are underway by Congress. We have a unique opportunity to, in fact, prepare while we repair our infrastructure. This is an opportunity that should not be lost as we move forward. It is an opportunity that can yield tremendous returns in minimizing impacts of future crises on our people and our economy.

The primary focus of this hearing without doubt is a specific risk, terrorism. In particular, Mumbai-style attack perhaps on a soft target in the United States. This committee has assembled a diversity of true experts in the terrorism risk and the specific strategies that would flow from that.

I would not pretend to approach their expertise, but I would suggest and stress that these specific risk strategies optimally are built upon a foundation of basic all-hazards preparedness, that this approach that acknowledges that many different risks can, in fact, have common impacts on people, property, processes; and that these impacts, these common impacts can be addressed by a set of core capabilities of an organization to essentially prepare, respond, and recover from crisis.

These core capabilities can be dramatically advanced by the Private Sector Prepared Preparedness Program called for by Title 9 Public Law 110–53.

The program essentially provides a set of common criteria, a standard for private sector preparedness, yet in a flexible framework. It provides a measurement or assessment approach to assure that criteria are in fact in place, and ultimately it provides the foundation or the opportunity to link compliance, conforming with those criteria with bottom-line impacts. It is that bottom-line im-

pact that will assure on-going and recurring investment by the private sector in preparedness.

Yet there are critical next steps that must be taken to assure that this program is successful. In particular, the Department of Homeland Security needs to, in relatively short order, designate one or more core standards as soon as possible to move the private sector preparedness certification program forward. The Department has already discussed the program with the private sector widely through a diversity of forums. Now is the time to move forward with one or more standards required by the legislation.

DHS should also continue to build upon and support the efforts of the designated accrediting body, which has a long history in certification and long interface with the private sector itself.

Furthermore, DHS should fund and work with appropriate stakeholders to support a mapping of industry-specific practices, best practices, if you will, in each of the major sectors using the common criteria of the Title 9 program as if you will, the Rosetta Stone that will allow us, once and for all, to begin to gather perspectives that may come from the elements of the private sector, including the hospitality industry, and including utilities, financial services programs, and begin to share these across sectors.

Furthermore, DHS should support the development and delivery of training to assist in implementing the criteria of the private sector preparedness programs. It should also support and fund the development and delivery of the appropriate tools to enable the implementation, including risk assessment methodologies online resources.

There are a diversity of resources out there and potential training available from various professional associations and nongovernmental sources. These should be capitalized upon and funded by the Department in this regard.

DHS should also support and fund a first wave of company certifications under the PS–Prep program. Participants should include high-profile opinion-leading companies, optimally with significant supply chains, and working with these suppliers, including both large, medium and small businesses. This will provide a proof of concept and an opportunity to test the program out on a small basis, if you will, and an opportunity to learn those lessons, to capture them, to inform a wider effort down the road, including, again, the critical small business community.

DHS should also fund and support what is perhaps the most long-term seminal impacting project. That is a research project that uses the measurements of the Title IX program to ultimately decide what the difference is, what the impact is of preparedness over time. There is no data currently on the impact of programmatic preparedness because, to date, there has been no effectively commonly accepted measure of what preparedness is, and there has been no commonly accepted approach to, in fact, confirm that those criteria are in place.

With the Title IX program, we have an opportunity to begin perhaps what is the first long-term effort to define the financial rationale that is the real value of investment and preparedness. Congress needs to continue its efforts, its active oversights of key program initiatives in this area, as evidenced by this committee's ac-

tivity. It also needs to fund DHS to accomplish the various initiatives that I briefly outlined.

Businesses need to look to the PS–Prep program as, at the very least, an informal internal assessment of their own activities, and over time, they need to look at it specifically for applications in their supply chain with the focus on supply chain resilience. They need to continue to actively partner with Government in information-sharing and public-private partnerships, and they need to consider being part of that first wave of company certifications under the new Private Sector Preparedness Program.

Finally, I would suggest that all parties need to look at the opportunity inherent in this new infrastructure program that is certainly being funded as part of the overall stimulus effort but to revisit this opportunity to prepare and repair as we move forward in substantiating and really rebuilding our infrastructure. Adding resilience to what essentially would be the considerations and the design stage for much of the existing infrastructure that has been targeted for rebuilding could pay tremendous dividends down the road, and a risk-assessment should and can be a standard step in advancing planning for all infrastructure projects, much the same as environmental impact studies have become in many other development efforts.

Our center stands ready to assist wherever appropriate and collaborate with all key stakeholders in the achievement of these critical initiatives. I thank you again for the opportunity to present to the committee.

[The statement of Mr. Raisch follows:]

PREPARED STATEMENT OF WILLIAM G. RAISCH

MARCH 11, 2009

Chairwoman Jackson-Lee, Ranking Member Dent, and distinguished Members of the subcommittee, it is my sincere honor to again provide testimony to this committee.

I join you today as past private sector advisor to the Federal 9–11 Commission and currently as Director of InterCEP, the International Center for Enterprise Preparedness at New York University. InterCEP is the world's first research center dedicated to private sector resilience.

In my capacity today, I am at best a channel for the many insights that are shared with the Center from hundreds of businesses and other organizations that participate in InterCEP forums and initiatives.

Our primary goal at InterCEP is simple. We work with key stakeholders to identify, understand, and collaboratively solve real problems in the area of emergency preparedness, security, operational continuity, and risk management.

I will now outline what we see as the current challenge of private sector preparedness (with a particular focus on the hospitality industry), the opportunity provided by the new Private Sector Preparedness Program (PS–Prep) and then address urgently needed actions in this arena for both Government and business.

THE CHALLENGE

Preparedness can be generally seen as an effort to develop capabilities to prevent a hazard where possible (and feasible) and to mitigate the impacts of a hazard should it nonetheless occur including capabilities to respond and recover while maintaining continuity of core operations.

The significant law enforcement expertise assembled by this committee today can better comment on the specifics of appropriate prevention strategies for a Mumbai-style attack in the United States. Clearly such prevention strategies would likely involve effective public-private coordination in terms of advance warning and intelligence sharing, a heightened level of awareness among staff and customers alike

as well as a level of physical security generally only applied to VIP appearances in our country.

I would like to focus my comments today on "all hazards" emergency preparedness which should be, but often is not, the general foundation upon which specific strategies to address any new or evolving threat is built. At the center of all hazards preparedness is preparing for the often common impacts of emergencies with common core capabilities. It involves developing capabilities for such activities as on-going threat assessment and situation analysis, a clearly understood incident management structure, effective warning and crisis communications with employees and customers alike, basic resource management and logistics necessary to access needed supplies, targeted training and exercises as well as effective relationships and communications capability with public safety organizations. All hazards programs should be what we fall back on in the event of the unexpected.

Overall preparedness appears to vary greatly among businesses generally and key drivers appear to include the size of firm, experience with crisis, and presence of regulatory requirements.[1]

- Larger firms or facilities (with more overall staff and other resources) tend on the whole to be more prepared than smaller firms.
- Firms that have experienced a crisis or recurring threats tend to be more prepared than those that have not.
  - (For example, the well-established threat of room theft in hotels has resulted in the general addition of room safes and restrictions in some cases of who can enter guest room areas).
- Firms that have regulatory requirements for overall preparedness (e.g., utilities and financial services firms) tend to be more prepared on a programmatic basis than those that do not. Similarly, specific requirements for elements of preparedness (such as fire and life safety) are clearly prompted by regulation. Such codes play an important role in the hospitality industry.
- Availability of financial resources and expertise is always a limiting factor. Unfortunately, security and preparedness expenditures are generally considered by most firms to be "overhead" costs and these have been severely cut and likely will continue to be further eroded should economic conditions worsen.
  - In the hospitality industry this can be exacerbated by the franchise system, whereby major hotel corporations may manage properties but these are owned by their franchisees who may have to approve operating budgets. While issues such as life safety and food safety are considered must-do regulatory requirements and are an accepted element of budgets, security is often considered optional in nature.
- Even among the most prepared firms, research suggests that preparedness and security overall can be significantly improved. But to maintain even the current levels of preparedness will require sustained funding but the current economic environment is resulting in significant across-the-board cutbacks to the area of preparedness and security.

THE NEED

In large part, it can be argued that the current situation is due to a lack of a clear "what" to do, "how" to do it and a compelling "why" to do it. In line with our prior testimony to this committee, several factors contribute to this situation primarily focused on these three considerations:

- *What to do*.—A set of clear criteria for what constitutes effective preparedness and security is needed. The criteria for what good preparedness is can be difficult to ascertain. There are a diversity of strategies, technologies, and approaches to preparedness and effective security. Most firms are not aware of any standards in this regard.
  - The criteria must optimally be derived from the private sector and based upon actual business experience to assure that it is applicable in the business environment.
  - Current successful industry practices must be acknowledged and built upon, not displaced. As with a number of other industries, the hospitality industry has significant history internationally as well as domestically in the security and preparedness arena; this experience should be at the core of any effort.

[1] While there is still no consensus-based measurement of preparedness for the private sector (pending the implementation of PS–Prep), we can draw on personal observations, anecdotal information, and what might be considered indicators of preparedness elements, such as surveys of expenditures on security or the presence of certain plans or programs. From these inputs, overall assertions can be made.

- *How to do it*.—Implementation strategies including risk assessment methodologies, training, and planning resources are necessary to apply the general criteria to specific business facilities/operations. "How" preparedness criteria (if identified) should be applied to a particular operation may not be clear. Size, geographic location, type of industry, current intelligence, etc. all can inform the nature of preparedness actions to be undertaken. Likely a small motel along an interstate does not require the same approach as a large hotel property next to an iconic building in a major city. How should risks be identified and prioritized? What training is necessary? What resources are available to support planning and implementation?
  - A risk-based methodology that can identify and prioritize risks and inform prevention, preparedness, response, and recovery activities is vital.
  - Appropriate training and other tools necessary to develop and implement preparedness programs on a company basis are needed.
  - Public-private partnerships in information sharing and intelligence with an emphasis on actionable information must be sought.
- *Why to do it*.—A compelling business case and the development of new incentives for preparedness with linkage to the common criteria is needed. The business case for preparedness is not always evident. Preparedness requires investment of time and resources. Businesses invest in efforts that increase profitability. It is not apparent to most businesses that an investment in preparedness will either increase revenue or decrease expense. The probability of hazards and their potential impacts on a business are difficult to assess. The perception that "it's not going to happen to me" is widespread. Thus, unless there are clear bottom-line reasons or regulatory requirements for preparedness and security, activity in this area tends to be minimal.
  - An approach is needed that does not rely solely on the risk of terrorism as the primary motivator (which will likely be discounted by many) but rather looks to the common impacts of many different risks on an operation and focuses on common strategies of preparedness, response, and recovery which can be established at a relatively lower cost than developing a number of individual risk-specific programs.
  - A serious and on-going research effort must be developed that not only documents current anecdotal impacts of preparedness but also develops new approaches to more comprehensively clarify the economic benefits of preparedness to the corporation and wider society.
  - The active engagement of key stakeholders in the development of new incentives must be promoted and maintained.

AN OPPORTUNITY: THE PRIVATE SECTOR PREPAREDNESS PROGRAM

The new Private Sector Preparedness Program (PS–Prep) championed by this committee and reflected in Public Law 110–53 holds great promise in addressing a number of these needs. It is as you know, currently under development by DHS. Key elements of the program include the following.

- The program is to be based on existing business preparedness standards by the private sector based upon its experiences over time, not by Government.
- The program will be risk-based. All of the standards in this arena require as a starting point a risk assessment and thus would suggest activity appropriate to the risks identified for each operation and not a one-size-fits-all approach.
- Core standards in the arena also incorporate cost-benefit analysis as part of their processes. Thus, firms are encouraged to prepare reasonably and to the extent allowed by available resources based upon true business value.
- The program is poised to be link preparedness over time with potential benefits and incentives. InterCEP currently has five Working Groups involving approximately two hundred individuals providing input on linkage to potential incentives over time in supply chain management, legal liability mitigation, rating agency acknowledgement, more rationalized business reporting on preparedness and insurance.

Nonetheless, the PS–Prep Program is only an element of a more comprehensive strategy needed to secure our businesses in general and the hospitality industry in particular. Additional elements are included below.

CRITICAL NEXT STEPS

There are several critical steps necessary to move forward preparedness within the private sector as a whole including the hospitality industry. Critical next steps must be taken by the Department of Homeland Security, Congress, and businesses.

The U.S. Department of Homeland Security (DHS):

- DHS must designate one or more core standards as soon as possible to move the PS–Prep certification program forward. While promising, this program is far from complete and the designation of standards is a necessary precursor to further activity. The Department has discussed the program with the private sector widely through a diversity of forums. It has developed and vetted its target criteria for the choice of standards and announced them publicly in the Federal Register. It has held two highly interactive national meetings with the private sector on the program. Now is the time to move forward and designate the one or more standards required by the legislation.
- DHS must continue to support the efforts of the designated accrediting body, ANAB, to assure that this program has a firm base in the historically proven private sector voluntary accreditation process. ANAB has administered accreditation programs in such areas as quality management (ISO 9000) and environmental management (ISO 14000) for decades. It has established relationships with the business sector and a time-validated approach to conformity assessment of businesses.
- DHS must support an outreach to the critical infrastructure sectors to engage them in the on-going development and implementation of the PS–Prep Program. These sectors are vital to a resilient society and they often have a well-developed appreciation of the importance of resilience. This outreach must:
  - Educate these sectors on the opportunity presented by certification program.
  - Clarify the program as an opportunity to identify and credit best practices already existent in each sector and not an effort to supplant existing and effective practices where they exist.
- DHS must fund and work with appropriate stakeholders to support the mapping of existing industry specific practices in preparedness and security, especially those in the critical infrastructure sectors. The common criteria of the new certification program offer a unique opportunity to identify and categorize good practice in these sectors.
  - Such a mapping could be used to assist in crediting these practices in the PS–Prep Program, so that those industries and companies with strong preparedness programs would be appropriately recognized.
  - Furthermore, and perhaps more importantly, this mapping could create an opportunity to cross-walk practices across industries allowing for cross-pollination of approaches and strategies. Such an effort could create a "rosetta stone of preparedness" which could establish a more robust body of good practices for all organizations. InterCEP is actively looking to engage with key industries in this regard.
  - Given the importance of the hospitality industry and its history to date, this industry could be one of the initial targets for collaboration on a mapping of existing practices.
  - DHS should coordinate this effort but consider that the outreach might best be undertaken in conjunction with non-governmental parties to minimize potential concerns about creeping regulation.
- DHS must support and fund the development and delivery of training to assist in implementing the common criteria of the PS–Prep program. Key professional associations should be considered for this effort including the American Society for Industrial Security (ASIS), Disaster Recovery Institute International (DRII), the National Fire Protection Association (NFPA) and the Risk Insurance & Management Society (RIMS).
- DHS must support and fund the development and delivery of appropriate tools to enable implementation including risk assessment methodologies and on-line resources. Risk assessment tools such as RAMCAP Plus (developed by ASME–ITI) should be considered. On-line resources such as the DHS Ready.gov site, the Open for Business® planning tool offered by the Institute for Business & Home Safety (IBHS) and the Red Cross Ready Program from the American Red Cross should be considered.
- DHS must support and fund a first wave of company certifications under the PS–Prep Program. Participants should include high-profile, opinion-leading companies with significant supply chains as well as their suppliers including small businesses.
  - This will provide a proof of concept and an opportunity to test the program out on a small scale before being rolled out on a wider basis.
  - Lessons learned can be captured and used to inform the wider effort, including lessons for both large and small businesses.
  - Leading corporations can both become familiar with the certification program (on a pilot basis) as well as provide high-profile leadership.

  - By including corporations with significant supply chains, these initial undertakings could set the foundation for supply chain-focused resiliency initiatives underscore a clear economic rationale for preparedness among small businesses. Such efforts could involve larger corporations working with a targeted group of their critical suppliers. In various InterCEP forums, several leading corporations have already indicated their interest in potentially mentoring their key suppliers in preparedness.
  - This first wave initiative should be funded by DHS and potentially utilize the DHS grant mechanism.
- DHS must support and fund a long-term seminal research project to begin to measure the economic value of preparedness over time. This project could ultimately provide the most compelling rationale for widespread investment by the private sector in resilience. There is no data on the impact of programmatic preparedness because prior to the inception of PS–Prep there has been: (a) No commonly accepted definition of what constitutes effective preparedness and (b) no method to measure if these preparedness criteria were in place. Lacking these fundamental elements (a definition and a measure), there has been no ability to see if prepared companies fare better after emergencies occur versus those companies that are not prepared. This lack of data has kept preparedness as a common-sense strategy but one that lacked any financial rationale that informed the real value of investment in preparedness. Hence, corporate efforts have tended to be notional and other actors such as insurance and rating companies have failed to strongly acknowledge and reward preparedness. They have lacked any real actuarial data on this vital area. With the PS–Prep Program in place, a long-term project can now be undertaken to identify different outcomes over time based upon whether or not a firm is "prepared" as indicated by its PS–Prep status. InterCEP seeks to be instrumental in this undertaking.

Congress:

- Congress must continue its active oversight of key programs and initiatives. Congress' wide perspective on this arena is critical to a comprehensive and sustainable strategy for private sector and overall society resilience.
- Congress must fund DHS and other stakeholders as appropriate to enable the above initiatives including the accrediting body required by the legislation, the mapping of existing industry practices to the common criteria of the designated standards, training and tools necessary to implement preparedness, the first wave of company certifications under the PS–Prep Program and the long-term research initiative.

Businesses:

- Businesses must look to the PS–Prep program for voluntary guidance and, as a first step, undertake an informal internal assessment of their operations based on the criteria of the program. Core to this will be an initial risk assessment to inform what preparedness measures are appropriate. Further application of the PS–Prep program should be considered if it presents additional business value.
- Additionally, businesses should evaluate the use of the PS–Prep Program in assuring supply chain resilience, especially for suppliers of mission critical services to core business operations. Firms with high priority needs and regulatory requirements for continuity such as the utility and financial services industries should especially evaluate this opportunity to assess the resilience of their critical suppliers.
- Businesses must actively partner with government in information sharing and other public-private partnerships. Information gained from these partnerships can inform risk assessment as well as other preparedness, response, and recovery activities. Federal programs include DHS Sector Coordinating Councils, DHS Information Sharing & Analysis Centers (ISAC's), DHS Protective Security Coordinator Division, FBI InfraGard, U.S. State Department Overseas Security Advisory Council (OSAC). State and city programs such as Chicago First, NYPD Shield, New York City Office of Emergency Management CorpNet/PALMS and the wide diversity of others should be considered. Private not-for-profit organizations such as Business Executives for National Security (BENS) should also be considered.
- Businesses should consider participation in the first wave of company certifications under the new Private Sector Preparedness Program.
- Businesses must promote and participate in an industry-by-industry effort to map and recognize existing preparedness and security practices utilizing the criteria of the PS–Prep certification program as the organizing theme.

Finally, all parties must work to assure that resilience is designed into our Nation's infrastructure projects from the beginning (not added after a crisis). We must

prepare as we repair and expand our infrastructure. The private sector and Federal, State, and local governments must take constructive action to assure this.

- Our goal must be to create a more resilient Nation as well as a better supported one.
- Adding resilience considerations at the design stage can generally be done at minimal costs. Yet, resilience can pay big dividends in reducing the cost of future disruptions that are inevitable due to both natural and man-made hazards.
- Risk assessments should be a standard step in the advance planning for all infrastructure projects. Such risk assessments could lead to designing in appropriate mitigation and prevention measures for identified hazards as well as measures which could facilitate response and recovery in any crisis, large or small.
- Existing strategies should be utilized to advance resilience including the both programmatic standards such as those under the PS–Prep program as well as risk assessment tools such as RAMCAP Plus.
- Infrastructure projects should consider local, State, regional, and Federal preparedness planning.
- In addition to protecting our people, a more resilient infrastructure will make for a more competitive America in the global marketplace.

Our Center stands ready to assist wherever appropriate and collaborate with all key stakeholders in the achievement of these critical initiatives.

Ms. JACKSON LEE. We thank all the witnesses for their testimony, and we will begin questioning the witnesses.

I will yield myself 5 minutes. We thank them for their testimony.

It would appear that, in the quietness of this room, we have nothing to fear. The reason that is so, because in the, if you will, in the emergence after 9/11, we began to wake up and understand the issues of terrorism and protecting the homeland. We are grateful to all the witnesses for recognizing their role in that. So we have, in fact, warded off, stopped, if you will, pressed back terrorist acts on our soil.

But I think that if we have not gotten a wake-up call over the last series of years, noting the numbers of terrorist acts that have occurred on trains, the ones that were attempted on airplanes, the ones that have been attempted in settings like hotels and sports events, then I think we are not getting the wake-up call that we should.

Let me start with you, Mr. Raisch, because you made a very interesting point. How long has Title IX been law?

Mr. RAISCH. I believe it was August 3, 2007. That would make it roughly, what, 1 year and 6 months roughly, 6 or 7 months.

Ms. JACKSON LEE. Enough time, if we were unlucky to have a number of terrorist acts, if that was what terrorists intended to do in the United States, and we were not prepared. Is that not right?

Mr. RAISCH. Certainly.

Ms. JACKSON LEE. So your point is a point that I think should be made very clearly. In that Title IX, I understand it was established a Voluntary Private Sector Preparedness Accreditation and Certification Program. Why don't you restate for us your point about the actions of the Department of Homeland Security from 2007 in terms of moving forward on reaching out to create, if you will, action on that voluntary accreditation certification?

Mr. RAISCH. To be fair to DHS, there have been significant actions on their part. At the same time, and over the course of that period of time, there has been outreach by the Department. There has been diversity of meetings. Most recently, two public forums were held in January and February of this year.

Ms. JACKSON LEE. Where were they held?

Mr. RAISCH. They were held in Washington, one at the U.S. Chamber of Commerce and the second one at the American Red Cross Headquarters here in the District of Columbia. There have been, my understanding, though, some outreaches. We participated in hosting a number of them whereby DHS has tried to get the word out.

Ms. JACKSON LEE. So what have been the obstacles of moving forward almost a year and a half to be able to establish the program?

Mr. RAISCH. I think the remaining obstacle right now, quite frankly, is simply designating a standard and/or standards. The legislation itself calls for one or more standards to be designated. That, quite frankly, with a year, 6, 7 months into it, we are beginning to lose potentially some momentum in that regard. I think DHS has made a concerted effort to outreach and vet. I think that vetting has been done, and I think it is time to move forward in that regard.

I think the private sector is ready to move forward. I think there has been input from a diversity of associations. There has been some very good work done by the Alfred P. Sloan Foundation. We brought together four major entities, professional entities in this case, and they have chimed in on it. We have heard InterContinental really speak about their use of the program, even in its infancy. As such, I think we are ready to move forward.

I think this needs to be a step progression, though. I think moving forward involves, first and foremost, designating the one or more standards. But then let's move out and in a logical progression, I think, the possibility of some pilot or first-wave projects.

Ms. JACKSON LEE. I think we need to move out, if you would, beyond the Beltway and establish some meetings on that issue as well.

The point that I think I would like to make in that is we recognize that there has been a new administration, changing of leadership. But I intend to and hope my Ranking Member will join me on encouraging, by way of letter, DHS to move forward on the characterization of the standards.

I would like to ask Mr. Bonnell, just to follow up in the line of questioning, would InterContinental seek to be certified and accredited?

Mr. BONNELL. Yes, ma'am. We in fact have applied for a Safety Act Compliance Certification. We are in the application process now.

Ms. JACKSON LEE. Let me move forward, Mr. Bonnell, and since I am going down the line, and thank you very much for representing a hotel family, is that not correct?

Mr. BONNELL. That is correct.

Ms. JACKSON LEE. So you are separate and apart; you are a member of the Hotel Association, but you actually represent active hotels.

Mr. BONNELL. That is correct.

Ms. JACKSON LEE. In the course of the council that has been set up, the commercial council, the DHS Commercial Facilities Sector Coordinating Council, are hotels actually sitting on as members?

Mr. BONNELL. We are on the Real Estate Roundtable committee.

Ms. JACKSON LEE. Alright. That is an interesting name. Are you sitting on the Commercial Facilities Sector Coordinating Council?

Mr. BONNELL. No, ma'am.

Ms. JACKSON LEE. Do you have a representative on that council?

Mr. BONNELL. My company does not directly. I think through the American Hotel Lodging Association we do have participation indirectly.

Ms. JACKSON LEE. I don't know the semantics, but I am much more comforted by the fact that you would be on the Commercial Facilities Coordinating Council than I might be on real estate. There must be something in that real estate name that someone attributes to covering the issues that we are concerned about. But let me just ask you the question. Is there too much money? Can we say that there is ever too much money invested in security?

Mr. BONNELL. No, ma'am.

Ms. JACKSON LEE. Particularly in commercial facilities.

Mr. BONNELL. Absolutely not.

Ms. JACKSON LEE. Can we be partners in helping commercial facilities be more security wise?

Let me indicate, as I said before, I stayed at the Taj, and so I understand what the post-November 26, what the description that we have heard of the commandos going through hallways. The question is, how much invasion of privacy are hallway cameras, for example, safe places, training staff on how to act? There were some heroic actions by hotel staff, and let me commend the hotel industry, saving, if you will, the clientele, those who were in the hotel as actual customers, not only of the restaurants but elsewhere, actually saving them, moving to their own safe spots. What is too much? What do you want from the Government in terms of assistance?

Mr. BONNELL. Well, I don't know how I can say what is too much.

I would say, to address some of the points, cameras in hallways are not intrusive. There is no expectation of privacy, and in many of our hotels, we strongly recommend the use of CCTV where appropriate.

In terms of training, you can't do enough. I will say this: The Department of Homeland Security, the U.S. State Department has been a tremendous source of information in developing training programs. For us, half of all knowledge is knowing where to find it. If I have questions about vendors, products, procedures, methods, I can go to these sites, the Web sites.

Ms. JACKSON LEE. This is DHS?

Mr. BONNELL. DHS, OSAC, and NYPD Shield. Tremendous sources of information. As I said, our security, and our counterterrorism programs are all intelligence-led. As hotels are being built, as the luxury class, full-service hotels are being built, we are now incorporating security design in the engineering phase, and we are making a requirement, both company-managed and franchise properties. So we are changing the way we are building hotels.

Existing properties, we have to do the best we can. But again, could we do more? Could we get more from the Government? I would certainly welcome any support. Again, for us, it is intelligence. As the Commissioner said, no two hotels are the same. So

it is hard to come up with a one-size-fits-all solution to security. We talk about the hotels that sit on waterfronts, that, similar to the Taj, unique set of threats, as opposed to say a hotel located in Phoenix. It is, again, when we go to addressing the issues of security, we have to look at what is reasonable, what is foreseeable, what is predictable.

Now as terrorist attacks against hotels have become more sophisticated, it is apparent that there are certain things that we should invest in. Again, talking about the performance of security personnel, for instance, the case at Islamabad, over 20 security officers were killed at the Marriott Islamabad. You will find that in many of the attacks, the security personnel are doing a good job, particularly those that are properly trained to look out as part of a counterterrorism program.

Ms. JACKSON LEE. Well, we thank you for that explanation.

With that, let me yield to the gentleman from Pennsylvania, Mr. Dent, for his questioning.

Mr. DENT. Thank you, Madam Chairwoman.

Thank you all for being with us this afternoon. Media reports coming out of Mumbai indicate that the LeT attackers had conducted significant surveillance prior to carrying out those attacks, so that they had an in-depth knowledge of the layout of the targets, even better than that of the first responders. This is a general question. You all feel free respond this. Is the U.S. private sector in a position to recognize pre-attack surveillance and report to Federal authorities? Anybody want to take a shot at that?

Mr. BONNELL. If I may, that is part of our counterterrorism program, when we train people to look out, to look at these points where the terrorists are going to be conducting these surveillance. We know from past attacks that they do counter surveillance and they invest heavily in counter surveillance, so we train our people to be on the lookout for it. In fact, there is an initiative underway now where hotels, different brands are sharing information, where we are watching each others' hotels, essentially watching each others' backs in areas where we have high concentrations of hotels that are close to each other.

So your point is absolutely spot on with our approach to counterterrorism is to train our line-level employees to be looking out and looking for the obvious indicators of counter surveillance. If you are being surveilled, if you look for it, you will see it.

Mr. DENT. Anybody else want to make a comment?

Mr. RAISCH. I guess I could chime in there. In prepping for this discussion here, I had the opportunity to reach out to a number of chief security officers in various hotel chains, and my understanding is it is definitely evolving. I think I was astounded by most of them I spoke to had at least one of their staff, if not themselves, had been in short order out to India and had done some post-event analysis out there. My understanding is there is an outreach to a great extent to the back to the house right now where they are trying to develop essentially posters that would reinforce suspicious activity, what cues would be in that regard. So I think it is evolving. I think there is some good work being done across the industry.

The interesting thing about preparedness is that sometimes an industry will collectively look at issues that otherwise might appear to be competitive because they have realized that if one attack occurs in the United States at a single hotel, people won't differentiate what flag is on that hotel. They will become increasingly cautious about all hotels. So I think we have a foundation for collaborative effort without question.

Mr. DENT. Finally, I just want to make a comment. Do high-priority targets in the U.S. private sector adequately train and exercise with first responders or provide critical information to first responders in the event of some kind of an attack, in your view?

Mr. Bonnell.

Mr. BONNELL. Do we train with first responders? We do. More so in some markets than in others. For instance, take Orlando, because of the high concentration of high-end hotels, we work, in fact, I know the regional coordinator for the Department of Homeland Security there who makes available resources for training. So I would say that does take place. For instance, in New York, we have the Barclay and the Crown Plaza Times Square, both security directors are retired NYPD police detectives, work closely with the local authorities. New York is really probably gone a step above as far as preparing for a crisis in terms of being certain the first responders are trained, that we know exactly where the ambulances and the fire trucks are going to come and the people know exactly what their assigned duty stations are. I would say in some markets more so than others.

Mr. RAISCH. If I could elaborate, I would also say this, and I would hope Mr. Bonnell would concur with me. There is a stratification in the industry. You have the major players in major, you know, certainly the larger hotels in larger cities tend to be the ones where there is more staff and arguably more cash-flow to rationalize much of the investment. There is a different level of staffing. There may be three people in a roadside, an interstate-side size hotel, and consequently, your capability to have a significant security presence there is minimal.

But I think the core approach to preparedness that I think I heard from Mr. Bonnell here was something that you can roll out through large and small entities and at least have the threshold level of preparedness and security even at the relatively smaller entities.

Mr. DENT. Thank you.

At this time, I have no further questions.

I yield back the balance of my time. Thank you for your testimony.

Ms. JACKSON LEE. Thank you, Mr. Dent, for your questions.

The Congresswoman from Nevada, Ms. Titus.

Ms. TITUS. Thank you very much, Madam Chairwoman.

My last question yielded little more than a mouth full of bureaucratese, but I am going to try again with this panel, so I appreciate your indulgence.

I would just ask you, either in your family of hotels or in your study of hotels, if you have looked at those that have gaming. You know, there are special needs when you have gaming. Your lobby is a casino. They are built in such a way that you can't find the

door. We want you to come in, but we don't necessarily want you to leave. So that makes it difficult. There are no clocks, there are no water fountains. It is a different setting. So I wonder if any of the study that you have been doing or any of the standards that you have been setting take into account those special needs.

Second, I want to be sure that everybody has the information and knows the best practices. I know the security forces do. I know the executives do. But what about the cocktail waitresses? What about the card dealers? What about the ladies that make the beds? Is that information getting down? Is it available to the public? Would they know where to go, where to stand to be rescued like you used to know where to go with a fire, if you had a fire, and what elevator not to take?

Finally, I would just ask you if you were going to rate how prepared the private sector is, especially in terms of hotels, how are we today on a scale of 1 to 10?

Mr. RAISCH. I will yield to my industry colleague here.

Mr. BONNELL. Well, let me say, having been at the 30th floor of the Bellagio during an earthquake, I had an opportunity to watch the hotel deal with the crisis, and it was clear they were prepared. They knew what to do. Again, this was a shelter-in-place situation, as opposed to an evacuation. What is unique about Las Vegas is you have these hotels with 3,000 rooms, versus a hotel with maybe 300 rooms; generally better staffed in terms of security, emergency medical personnel that are actually on staff. So what I find in Las Vegas and in Reno is a very high level of preparation for crisis.

Now, traditionally, the investment in security had been in the casinos. As the super hotels came along, and they became victim, fell victim to premise security liability litigation, they found themselves in court, being sued for negligence, they began to increase the level of operational security on the hotel side.

Having been involved, through the American Society of Industrial Security, with the Gaming Committee, I tend to think the hotels that I have seen in Reno and Las Vegas are superior in many respects because, again, I think they anticipate these events occurring. That is from my own personal knowledge. I haven't conducted a study. I am more familiar with hotels in the range of say 350 to 750 rooms, business and leisure, so I am not well versed in casino.

Again, I think you draw a unique set of threats associated with casino more in terms of criminal behavior. Again, as I said, when I saw the folks at the Bellagio and the MGM Grand respond to the earthquake, I was very impressed with their knowledge of directing people. In fact, they were actually at the bottom of the elevator banks with robes because they knew that people were going to come fleeing out of the rooms in their night clothes. So I was very impressed with that.

The other question—how do we rate? The hospitality industry is highly regulated. We have to deal with OSHA, ADA, NFPA, the constant threat of litigation in the form of premise security liability lawsuits. Our insurance carriers want to make certain that we are managing our hotels in preparation for these foreseeable risks. So I would say, compared to say, retail, we are doing pretty good. I can't say, I don't want to say that we are doing a lot better, but I think that because we are held to a higher level of accountability

than say our colleagues in retail, we do a better job overall. But of course, when people check into our hotels, they are trusting us with their lives and their safety. And generally we have much longer contact with them. So I would be reluctant to give us a score. I would say C-plus, maybe a B-minus.

Mr. RAISCH. It is my hope in 2 years hence that that question of what level is security and preparedness at hotels can be met by giving you a number as to how many have actually been certified under the program. That is inherent really in one of the goals of the program is to provide some measurement and common criteria because, to date, what your concept of preparedness is or mine or any one of the folks on the panel in this room, none of them would exactly jive.

In this case, we have the opportunity to look at some bubble-up standards that have come from the industry, not arbitrarily chosen in the Beltway, and to begin to apply those and evolve them. Each of these standards are not frozen in time. They actually have committees that maintain them on an on-going basis, so they will adjust over time to other threats as they evolve, perhaps along the lines of the Mumbai attack. So I think there is an opportunity inherent in the Title IX program to begin to measure that.

As we often know in many cases, until you measure something, it is very difficult to manage it. So my sense is that that is a strong opportunity really for the Title IX program.

The other observations we have made essentially is, obviously, as I mentioned before, larger firms with more facilities, larger, in this case, larger facilities with more staff, distinct from larger firms, because we have in this industry a stratification of everything from 30-, 40-, 50-, 60-unit hotels to 500- or 1,000-unit hotels, each of them with different staffing levels, each of them following different pricing mechanisms.

One factor that I did, became apparent to me, is the franchise system. We have the opportunity here to talk to, if you will, one of the major flags, InterContinental. While they manage the hotels, they don't necessarily own them, and their operating budgets are oftentimes approved by the local owners. Unfortunately, on the regulatory side, fire was mentioned before, OSHA, and so forth, there is a given in every budget for that number.

The security side is a little bit more iffy, and as such, oftentimes, I think security professionals like at this table have to, if you will, make an argument to the local operators, sometimes successful, sometimes not successful in what level of security that they are willing to buy into.

Ms. TITUS. Madam Chairwoman, thank you.

I think that Las Vegas does do a good job and has some things to offer, especially that they have developed. So I hope, as you develop these standards and this certification program, that Las Vegas can play a part in helping to flesh out some of that.

Thank you, ma'am.

Ms. JACKSON LEE. Madam Congresswoman, we hope to certainly involve your constituents who certainly have had their experience with large volumes of customers and revelers, if you will, and that is a question that we ask today, is to move quickly on the standards being, if you will, being put in place. So we thank you for that

offer. I know that the committee will take up both your advice and counsel.

I am going to seek to yield myself 5 minutes just to conclude. I don't know if Mr. Dent cares for that at this time, but I want to clear up some issues that are on the record.

Dr. Fair, you have mentioned radicalization and LeT. I want to make sure you are not suggesting that the people of Pakistan are comfortable with terrorist acts and are not making efforts. I was in Pakistan as well, post the November 26 incidents, and I know that, though it might not have been fast enough, they have come to recognize that there were Pakistani nationals participating. They have made a commitment to prosecute them, hopefully swiftly. Of course, they have themselves been victims of terrorist acts, including the issue dealing with the Marriott at Islamabad.

So my question to you is, how can we be effective in collaborating with our world partners when terrorism is becoming both decentralized and radicalized?

Ms. FAIR. Actually, I want to respectfully disagree with I think some of the points that you just made. There is a tendency to think of this broad swath of militant groups as all being interchangeable. In my written testimony, I go to great lengths to talk about how Lashkar-e-Taiba is very different. Lashkar has never targeted the Pakistani state. Lashkar-e-Taiba has never targeted an international target within Pakistan.

Ms. JACKSON LEE. So what are you disagreeing with me on——

Ms. FAIR. No, no——

Ms. JACKSON LEE. Because all I said was that they were becoming decentralized terrorist groups so that they are decentralized from al Qaeda and radicalized. Those are just the two points that I made.

Ms. FAIR. The part in particular that I think is an important question that really requires vigilance on the part of Washington is actually the extent to which they are undertaking efforts to wrap up Lashkar-e-Taiba. I personally——

Ms. JACKSON LEE. Who is "they"?

Ms. FAIR. The Pakistani government. I was not—there is a pattern that has been followed here as has been followed in the past; that is, before the organization is officially proscribed, the moneys in the bank accounts are moved, and the organization reconstitutes under another name.

The leader of the organization has not been arrested. He has been under house arrest. There have been a number of individuals who have been detained. Their actual accounting, the accounting of where they are is absolutely unclear. I was actually not impressed that the Punjab government, the provincial government, simply took over——

Ms. JACKSON LEE. Is that the state government?

Ms. FAIR. The state government. The state government took over the assets of an organization that the government itself had declared to be a terrorist organization.

What government takes over the operating of enterprises associated with a terrorist organization as opposed to shutting them down and arresting the leadership?

So I think there are a lot of questions, particularly about Lashkar-e-Taiba.

Ms. JACKSON LEE. How can we be more effective in collaborating with countries that have sovereign governments who represent that they are trying to fight terrorism and to be effective?

Ms. FAIR. Well, I think we have to be very forthright with them, both publicly, if need be, but certainly privately. Over the last 7 years the United States has really given Pakistan a mixed message about the groups that we think it should shut down.

For much of the global war on terrorism, we emphasized al Qaeda. We were actually very episodic in our emphasis upon groups like Lashkar-e-Taiba and Jaish-e-Mohammed. I am sure, as you know from previous testimony on the Hill, we were even ambivalent about Pakistan's efforts against the Talibans.

So I think the first thing that we need to do is resolve in our own discourse that groups like Lashkar-e-Taiba are not simply India's problem, but they are also our problem, and they are also Pakistan's problem.

Second, we really need to focus much more intelligence resources to really understand what the government is and, more importantly, what it is not doing. We have a tendency to look at these attacks through the optic of as if it just happened, and we tend to forget that in fact this group has been operating since 1986, and there is a pattern of state behavior with that particular group.

Ms. JACKSON LEE. I think your point is well taken, but we also need to distinguish what is state government and what is federal government in the context of Pakistan. We also need to be assured that we promote and encourage those efforts where the government is trying to at least work on a plan or an effort to fight terrorism.

I think the point is well taken. I think, in addition, we would hope that there would be notice, as I think your testimony said, that there were Indian facilitators. So working regionally, with India, Afghanistan, and Pakistan, I hope would be also an important point for us. But I thank you very much for your testimony and those very vital points.

Mr. Bonnell, let me ask, you want to certify under the SAFETY Act. But you would be willing to have InterContinental Hotel certify under the voluntary certification under Title IX?

Mr. BONNELL. Yes, ma'am.

Ms. JACKSON LEE. Do you think it would be helpful for DHS to reach out, beyond the meetings that they have already had, to really get, as Congresswoman Titus has indicated, sort of insight and instruction for hotels beyond the Beltway and be out in the areas, resort areas, for example, we have a lot of coastline in the United States, Las Vegas, for example, and other intense areas, do you think that would be helpful in terms of quickly moving and trying to establish some standards?

Mr. BONNELL. Yes, ma'am. I totally agree. I think that there are many best practices out there that we could share, work with DHS, consolidate this, and crystallize this information, and get it back out to where it would do the most good.

Ms. JACKSON LEE. I do want to emphasize, since I was physically on-site, using my somewhat non-, both nonscientific and non-law-enforcement eye, the importance of internal preparedness plans for

hotels. Though you represent one chain and one family, is there a standard, without the involvement of the Federal Government, where you would assess that hotels have their own individual plans? Are they wide enough to, for example, capture what Dr. Fair has said in terms of organizations that may be even beyond the borders of where we have seen them act out their terrorist acts? Are U.S. hotels with preparedness plans that could respond to a commando-type incident?

Mr. BONNELL. Limiting the discussion to the category and class of hotel that we have been discussing, again, like the Taj, the Oberoi or an InterContinental Hotel, you will find that there are plans. Is there a standard? Is there continuity and consistency? I don't think so. I can speak only to my brands. Now I work closely with my colleagues, with Starwood and Marriott, and we share information. I would say, within this small group of the major brands, we share best practices, and you would find some degree of continuity and consistency. But when you look at all of the hotels in this country, I am afraid the answer would be no. I think, again, setting a standard and providing and offering that standard up as a best practice would be very useful.

Ms. JACKSON LEE. I thank you very much.

Mr. Raisch, you have expressed the offering of your center's assistance and also your assistance for what has to be an important charge and challenge, and that is for the overall preparedness under Title IX, but in particular, establishing these standards. What is your sense of urgency on helping us move in that direction?

Mr. RAISCH. That is the designation, and let's make it clear, too, that really we are talking about designating existing standards that actually are bubbling up or have already bubbled up for some time for the private sector. So DHS need not create something in this regard. It in fact is charged by the legislation to designate an existing standard. So that is the opportunity that we have, not to attempt to build from scratch but rather to designate something that already has, again, come from the private sector. It is the next step that really is critical to move forward.

Absent a standard, really, the measurement process, the assessment process can't go forward absent one or more standards maybe designated by the Department in this regard. But that is the final element. Quite frankly, we are working on the bottom-line side of the house.

We have five different working groups over 200 organizations actively involved in it; that is, looking, once the standard itself has been defined, to look for benefits and insurance, mitigating legal liability, and acknowledgment by rating agencies and moving forward with really supply chain management where, perhaps, the most economic rationale——

Ms. JACKSON LEE. You are looking across the private sector in its totality, not isolating hotels. You are looking across the board.

Mr. RAISCH. We have representatives from utilities, from financial services, from the major retailers across the board, and all of them are really participating. The goal in all this is, by getting the private sector involved in it up front, we are essentially building something that is business and value-oriented as opposed to—we

referenced the Beltway before—building something in here and trying to make it work out there.

Ms. JACKSON LEE. If I had to ask the question on a scale of 1 to 10, with 10 being the highest, how would you rate the preparedness of America's private sector?

Mr. RAISCH. I would really hesitate to put a specific number because, quite frankly, the private sector is not a homogeneous entity. It is big, small, you know, large. Certainly the smaller businesses are more concerned about meeting payroll in the next 4 weeks than they are necessarily of putting their preparedness program together. I will tell you that those entities that have experienced some sort of crisis or near-miss, have gotten religion, those folks tend to be more prepared. We tend to see preparedness paralleling, at least on the life-safety side of the house—we reference NFPA and fire safety and life safety. There are elements of that because it has been required.

The typical business continuity and the more general elements of preparedness still are looking for something in the way of a definition as to what good preparedness is and a bottom-line rational to undertake it. That is why I think, once, if we link those two, which I think Title IX has the opportunity to do, not immediately but a little bit over time, then I think we will have the business rationale to make this go forward.

Ms. JACKSON LEE. Well, we certainly have an obligation to provide them that. But I imagine what you are saying is that they have not reached 10 yet.

Mr. RAISCH. There is no question in my mind they have not reached 10. I would say, on the whole, we are far; that is a long reach.

Ms. JACKSON LEE. I think you have given us our marching orders.

Let me thank our witnesses, of course, for their very instructive testimony.

Dr. Fair, Mr. Bonnell, Mr. Raisch, we appreciate the insight.

This hearing started off as I opened to connect the issue of the terrible tragedy in Mumbai with a wake-up call for America. Obviously, in order to fulfill the purpose of this hearing, we will be instructing and requesting certain responses from DHS of recognizing that we have a committed new administration ready to answer some of the questions that have been somewhat delayed.

We also will be actively engaged in pushing for the standard and certification process under Title IX. We welcome your input, and as well, we will be looking for a combination of working with intelligence committees, our foreign affairs committees, and this committee on the issue of terrorist groups, that Dr. Fair has mentioned and how do we be instructive with our allies who themselves are looking for a way out of the burden of terrorism. So let me, again, thank you for contributing to that.

Peter King mentioned a quote or a statement from one of our very famous newspapers that I tend to agree with all the time and has indicated we shouldn't be talking about terrorism. Well, we should be talking about terrorism and preparedness, because both of those, coming together, meaning prepared to fight terrorism and

being prepared will help to save lives, and that is what this committee is about.

I want to thank my Ranking Member, Mr. Dent, for his service. At this time, we will provide you with just a few instructive remarks and then the hearing will be adjourned.

The Chair wants to acknowledge that the witnesses have given valuable testimony. We thank the Members for their questions. The Members of the subcommittee may have additional questions for the witnesses, and we ask that you respond to them expeditiously in writing.

Hearing no further business, the subcommittee stands adjourned, and we look forward to submitting our questions. Thank you.

[Whereupon, at 5:23 p.m., the subcommittee was adjourned.]