AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

PARTNERING WITH THE PRIVATE SECTOR TO SECURE CRITICAL INFRASTRUCTURE: HAS THE DEPARTMENT OF HOMELAND SECURITY ABANDONED THE RESILIENCE-BASED APPROACH?

HEARING

BEFORE THE

SUBCOMMITTEE ON TRANSPORTATION SECURITY AND INFRASTRUCTURE PROTECTION

OF THE

COMMITTEE ON HOMELAND SECURITY HOUSE OF REPRESENTATIVES

ONE HUNDRED TENTH CONGRESS

SECOND SESSION

MAY 14, 2008

Serial No. 110–114

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

43–939 PDF WASHINGTON : 2008

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) 512–2104 Mail: Stop IDCC, Washington, DC 20402–0001

COMMITTEE ON HOMELAND SECURITY

BENNIE G. THOMPSON, Mississippi, *Chairman*

LORETTA SANCHEZ, California
EDWARD J. MARKEY, Massachusetts
NORMAN D. DICKS, Washington
JANE HARMAN, California
PETER A. DEFAZIO, Oregon
NITA M. LOWEY, New York
ELEANOR HOLMES NORTON, District of Columbia
ZOE LOFGREN, California
SHEILA JACKSON LEE, Texas
DONNA M. CHRISTENSEN, U.S. Virgin Islands
BOB ETHERIDGE, North Carolina
JAMES R. LANGEVIN, Rhode Island
HENRY CUELLAR, Texas
CHRISTOPHER P. CARNEY, Pennsylvania
YVETTE D. CLARKE, New York
AL GREEN, Texas
ED PERLMUTTER, Colorado
BILL PASCRELL, JR., New Jersey

PETER T. KING, New York
LAMAR SMITH, Texas
CHRISTOPHER SHAYS, Connecticut
MARK E. SOUDER, Indiana
TOM DAVIS, Virginia
DANIEL E. LUNGREN, California
MIKE ROGERS, Alabama
DAVID G. REICHERT, Washington
MICHAEL T. MCCAUL, Texas
CHARLES W. DENT, Pennsylvania
GINNY BROWN-WAITE, Florida
GUS M. BILIRAKIS, Florida
DAVID DAVIS, Tennessee
PAUL C. BROUN, Georgia
CANDICE S. MILLER, Michigan

JESSICA HERRERA-FLANIGAN, *Staff Director & General Counsel*
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*

EDWARD J. MARKEY, Massachusetts
PETER A. DEFAZIO, Oregon
ELEANOR HOLMES NORTON, District of Columbia
YVETTE D. CLARKE, New York
ED PERLMUTTER, Colorado
BENNIE G. THOMPSON, Mississippi *(Ex Officio)*

DANIEL E. LUNGREN, California
GINNY BROWN-WAITE, Florida
GUS M. BILIRAKIS, Florida
PAUL C. BROUN, Georgia
PETER T. KING, NEW YORK *(Ex Officio)*

ERIN DASTE, *Director & Counsel*
NATALIE NIXON, *Deputy Chief Clerk*
COLEY O'BRIEN, *Minority Senior Counsel*

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 Daniel E. Lungren, a Representative in Congress From the State of California, and Ranking Member, Subcommittee on Transportation Security and Infrastructure Protection 4

WITNESSES

Colonel Robert B. Stephan, Assistant Secretary, Infrastructure Protection, Department of Homeland Security:
Oral Statement 7
Prepared Statement 9
Mr. Jonah J. Czerwinski, Senior Fellow, Homeland Security, IBM Global Leadership Initiative:
Oral Statement 14
Prepared Statement 15
Mr. Shawn Johnson, Vice Chairman, Financial Services, Sector Coordinating Council:
Oral Statement 17
Prepared Statement 19
Mr. William G. Raisch, Director, International Center for Enterprise Preparedness, New York University:
Oral Statement 22
Prepared Statement 24
Dr. Kevin U. Stephens, M.D., Director, Health Department, City of New Orleans:
Oral Statement 30
Prepared Statement 33

PARTNERING WITH THE PRIVATE SECTOR TO SECURE CRITICAL INFRASTRUCTURE: HAS THE DEPARTMENT OF HOMELAND SECURITY ABANDONED THE RESILIENCE-BASED APPROACH?

Wednesday, May 14, 2008

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 2:22 p.m., in Room 311, Cannon House Office Building, Hon. Sheila Jackson Lee [chairwoman of the subcommittee] presiding.

Present: Representatives Jackson Lee and Lungren.

Ms. JACKSON LEE [presiding.] Good afternoon. Let me thank the witnesses for their indulgence. The subcommittee will come to order.

The subcommittee is meeting today to receive testimony on partnering with the private sector to secure critical infrastructure. Has the Department of Homeland Security abandoned the resilience-based approach?

Importantly, this testimony will discuss what the Office of Infrastructure Protection has done to promote the concept of resiliency throughout the 17 critical infrastructure sectors.

I am proud to convene today's hearing, which will focus on private sector participation in securing our Nation's critical infrastructure. Among our goals today is to determine the applicability of resilience to this mission, to what extent the Department is promoting it, and what we as a Congress can do to support these efforts.

At the outset, I wish to thank Chairman Thompson for declaring May Resilience Month for our committee.

In support of Resilience Month, today's hearing will focus on an area ripe with resilience-related issues. Perhaps nowhere is resilience more relevant to homeland security than the area of critical infrastructure protection, which I think could be more accurately termed critical infrastructure protection and resilience.

After the attacks on September 11, most of the record $80 billion in economic losses was suffered by the private sector. The consequences of Hurricane Katrina and Rita caused extraordinary damage, as well. The magnitude of the hurricanes' actual impact

was rivaled only by the catastrophic failure of the Federal Government to adequately respond to the resulting suffering.

I am proud to be focusing on critical infrastructure resilience, but I know that others have also advocated this position for some time. A task force of the Homeland Security Advisory Council on Critical Infrastructure released a report in 2006 stating that the focus should be shifted from protection to resilience, because it made a more convincing business case to companies.

I might add that we want to hear from those here today to find a way to balance protection and resilience. I believe we can.

The report said that resilience offers an effective metric—time—companies can measure how long it will be down in the wake of a particular disaster and can work to minimize that time. Resilience, I must say, is not capitulation, we in no way are saying that our guard should be taken down, to assert that we are mere political theater.

Instead, we are honestly saying to the American people that we cannot protect everything all of the time. So if we are hit or one of our suppliers is hit, we plan to ensure that we can recover quickly so grave damage is not done to our economy.

Our most recent examples—and we are very grateful that we have not had a terrorist attack since 9/11. We applaud all of the front-liners and certainly the Department of Homeland Security and the diligence of this Congress. But we also use as a backdrop of experience some of the tragedies that have occurred over the last couple of years.

For example, Hurricane Katrina is a prime example of the lack of resiliency. Who knows what will happen with the terrible excess of tornadoes that have occurred over the last couple of days and last couple of weeks and the damage that has been done to major geographic areas, including the obliteration or elimination of a whole city?

What is the resilience there? That is a very good example for us to use as a backdrop. What is the resilience in countries, of course, with different political systems? What will be the resilience of a China or a Burma?

These are questions that we should be asking so that we are prepared for what may happen to us here in the United States.

It is my belief that the Department should utilize resilience as a means of which to encourage private owners and operators to secure their infrastructure for three reasons.

It requires the provision of information that demonstrates to companies that there is an actionable threat to their infrastructure.

Most of the time, this information is not available and, as a result, companies do not see the justification of these expenditures in the absence of a threat.

Related to the first, companies have been trained by this economy to have no expenditures that do not produce profit within a few months. Protective and preventative measures to defend against a terrorist act likely do not generate such a profit.

Third, a focus on protection prevention is not measurable. We have no metric for quantifying whether something is protected. Without being able to quantify when enough is enough, industry is more reluctant to act.

However, I might issue a warning: Failing to do this, failing to do this is the storybook tragedy for failure and for a long, drawn-out journey of recuperation. Look to see how hard the people of New Orleans are working, but because of the failed actions of the Federal Government, resilience, recuperation has been long in coming.

A strategy based upon resilience is not a silver bullet, but it does support the critical infrastructure security objectives. Beyond encouraging preventative and protective measures, it asks companies to ensure that they can bounce back due to a disruption, which may include a terrorist attack.

This will support communities' supply chains and our national psyche. Furthermore, a focus on resilience can increase the profitability of our companies. For example, a 2007 report by the Council on Competitiveness, entitled "The Resilient Economy: Integrating Competitiveness and Security," asserting that the 835 companies that announced a supply chain disruption between 1989 and 2000 experienced 33 percent to 40 percent lower stock returns than their industry peers.

Those companies that were resilient, and thus able to effectively deal with and bounce back from disruptions, were the ones which grew in market share and saw increased returns.

In many ways, last week's full committee hearing was eye-opening. I do believe that the Department is doing more with resilience than was mentioned at the hearing. I look forward to hearing from Assistant Secretary Stephan about those programs under his auspices, and where and why, and why not, and he sees resilience as being more effective.

This committee has not shied away from promoting private-sector security. The 9/11 bill passed last August included a voluntary private-sector preparedness accreditation and certification program.

By no means is this program regulatory, but it does provide for a conversation between the Department and the private sector about security.

Led by Chairman Thompson, we included language that called upon the Department to work with Sector Coordinating Councils under Assistant Secretary Stephan to develop the standards for the voluntary program.

I look forward to hearing more about this program today and hearing whether the contemplated standards will include an element of resilience.

This subcommittee is not interested in blame or bashing. This subcommittee cares only about securing our critical infrastructure and having a constructive dialogue with the Department.

We believe that this hearing is a part of that dialogue and look forward to learning from Assistant Secretary Stephan and our other witnesses. Resilience may not be the silver bullet, but a real discussion about it may make us more secure in our days, weeks, months and years.

Who knows? There may be legislative penalties for those who don't see this as a constructive aspect of their business. We have to be able to save lives; we have to be able to save the economy; we have to be able to move forward during this time of crisis. To do so, we need the involvement of the public and private sector.

Once again, I would like to thank everyone for their participation today, and I look forward to hearing from each of the witnesses.

At this time, I would like to enter into the record the 2006 Homeland Security Advisory Council report on critical infrastructure. Hearing no objections, so ordered.*

The Chair is now pleased to recognize the distinguished Ranking Member of the subcommittee, the gentleman from California, Mr. Lungren, for an opening statement.

Mr. LUNGREN. Thank you very much, Chairwoman Jackson Lee.

Thank you, members of the panel, for coming here to testify. But more importantly, thanks for the work that you have been doing.

I certainly share the chairlady's interest and concern over the challenges this Nation faces to secure critical infrastructure. You probably know as well as anybody, those of you on the panel, it is an enormous job because of the thousands of critical infrastructure assets we enjoy, stretching from coast to coast and beyond.

Pursuant to Homeland Security Directive 7, the Department of Homeland Security developed the National Infrastructure Protection Plan, NIPP, to identify these vital assets and coordinate protection efforts across 18 critical infrastructure sectors.

Assistant Secretary Stephan, we thank you for the work that you have done in leading this effort on behalf of homeland security. Also, I recall when you came and asked for delay of its issuance until it met, by your judgment, the high standards that you thought were required.

By identifying critical assets and interdependencies, coordinating risk-based protection programs, and ensuring information, the NIPP provides the blueprint, I believe, for a safer, more secure, more resilient America. It sets national priorities, goals and requirements for effective distribution of funding and resources to help ensure that our government, economy and public services continue in the event of a terrorist attack or other disaster.

Because the private sector owns or operates approximately 85 percent of the Nation's critical infrastructure, partnering with the private sector is absolutely essential. To a great extent, we found the private sector has focused on ensuring its systems and networks were resilient and able to withstand disruption, manmade or natural, because of commercial and economic benefits.

I guess one of the questions we have is: How do we ensure that continues or, in those cases where it is tough to make it justified by the bottom line, how do we change the analysis so that people understand that to be important?

After 9/11, when the financial markets quickly resumed normal activity, Homeland Security began fostering public and private partnerships to perfect our country's critical infrastructure, with each sector bringing strength to the partnership.

The government provides access to critical threat information, and I think that is as important as anything else we do. If you don't have the proper information, it is very difficult to calculate what the threat is out there and very difficult for you to respond to that threat.

---

*The information has been retained in committee files.

The government also provides grants, which each sector controls its own security programs, research and development, and other resources that are more effective when shared.

Another example, I believe, of the Department promoting resiliency is the creation of the National Infrastructure Simulation and Analysis Center. It identifies interdependencies, the consequence of infrastructure disruptions, and suggests remedial action across all critical infrastructure sectors.

It just seems to me that the four key mission areas of the Department of Homeland Security—preventing, protecting against, responding to, and recovering from terrorist attacks or natural disasters—are equally important, whether we use the rubric of resiliency or not.

I would prefer to prevent an attack, as I am sure we all would, rather than respond and recover from one. However, if there is another attack or natural disaster, we must ensure that the Department and its governmental and private-sector partners can respond to and recover from such an incident.

So we thank you for being here. I look very much forward to the testimony from our witnesses.

If I were still chairperson, I would invite you to speak. But a funny thing happened on the way to the ballot box a couple years ago.

With that, I would yield back the balance of my time.

Ms. JACKSON LEE. The gentleman has yielded back his time.

I welcome our panel of witnesses. Our first witness, Assistant Secretary Robert Stephan, was appointed to serve as the Assistant Secretary of Homeland Security for Infrastructure Protection in April 2005. In this capacity, he is responsible for the Department's efforts to catalogue our critical infrastructure and key resources and coordinate risk-based strategies and protective measures to secure them from terrorist attack.

I would like to especially thank Colonel Stephan for his participation today. I understand—and he has been on and been between two international trips. I might say—I don't know if I want to say for the record, because he looks very well to me—but we will put it in the record so that he is covered. He is fighting off jetlag.

But he has always been very gracious in his relationship with this committee and the Congress but, more importantly, very dutiful and attentive to his responsibilities at Homeland Security. This committee recognizes and appreciates his dedication to the Department and this very important topic.

Our second witness is Mr. Jonah Czerwinski. Jonah Czerwinski is Managing Consultant, Global Business Services at IBM, and a Senior Fellow for Homeland Security in IBM's Global Leadership Initiative.

First, we are glad that the private sector has seen fit to establish such an initiative, and we look forward to hearing his testimony. He is responsible for developing policy, guidance for the global movement management campaign at IBM. He also served on the Council on Foreign Relations Study Group on Strategies for Defense Against Nuclear Terrorism.

From 2001 to 2004, he directed the center's homeland security roundtable, which regularly convened senior homeland security

leadership of the executive branch and Congress with leaders of the think-tank community, academia, and private sector to discuss critical homeland security issues. He is the primary contributor to the Homeland Security Blog, *www.hlswatch.com.*

Our third witness is Mr. Shawn Johnson. Mr. Johnson is a Managing Director of State Street Global Advisors. He is the Chairman of the SSGA Investment Committee and Director of Institutional Fiduciary Services.

Shawn is also a member of the State Street Corporation's Major Risk Committee, as well as the SSGA's independent fiduciary committee, and the SSGA Tuckerman Real Estate Investment Committee.

In addition to managing SSGA's team of economists and strategists, Shawn oversees SSGA's advanced research center, product engineering, as well as private equity investments, including CitiStreet, Wilton, ABCM, and SSGI Italy.

He is also responsible for SSGA's merger and acquisition activities globally. Additionally, Shawn is currently the Vice President of the Financial Services Sector Coordinating Council, the private-sector organization that coordinates homeland security issues with Federal and financial regulators.

We need not go any further than 9/11 to recognize the impact on the financial services industry, particularly Wall Street, to know how important the testimony is today.

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

His work with Intercep focuses on the development of actual strategies and policies in this arena through active engagement of key stakeholders. Topical concentrations reflect an emphasis on the what and the why of resilience and include best practices, standards, metrics, assessments, information flow, public-private partnerships, and the economic impact of resilience, including the role of incentives for business.

In addition to strong involvement with the U.S. business sector, the center has an international outreach actively working with a diversity of multinational corporations, as well as representatives from various national governments and NGOs globally.

You are welcome.

Our fifth and final witness is Dr. Kevin Stephens, Health Director for the city of New Orleans. He has served in this position since 2002. His responsibilities for public health in New Orleans include managing six divisions and 30 programs, encompassing a wide range of health issues.

Dr. Stephens served as Health Director both before and after Katrina and knows firsthand the importance of health care infrastructure resiliency.

Dr. Stephens serves on the clinical faculty of Xavier University, Dillard University, LSU Medical School, and Tulane Medical School. He is a member of the Louisiana Bar Association and has

worked as a consultant to many local and State and Federal agencies.

It is my great hope, Dr. Stephens, that as we know that you are certainly wanting to commend and celebrate the great progress that has been made in New Orleans—and let me, for the record, acknowledge that—I want you to be, if you will unabashedly forward and forceful on the state of the health infrastructure in New Orleans.

I will place in the record my appreciation and respect for the hard work that the people of New Orleans and the municipal leaders have engaged in. Today, however, we want the raw facts of where you are today.

So I welcome all of the witnesses. Without objection, the witnesses' full statements will be inserted in the record.

I now ask each witness to summarize his statement for 5 minutes, beginning with Assistant Secretary Stephan.

You are recognized and welcome for 5 minutes.

STATEMENT OF COLONEL ROBERT B. STEPHAN, ASSISTANT SECRETARY, INFRASTRUCTURE PROTECTION, DEPARTMENT OF HOMELAND SECURITY

Colonel STEPHAN. Thank you, Madam Chairwoman, Ranking Member Lungren. I appreciate the opportunity to be before you today.

I also appreciate your ongoing leadership and focus in this very important subset of the homeland security overall mission area. I know you have heard previous testimony from some of my department counterparts, as well as key private-sector stakeholders, on this topic.

I also hope from my heart that you received a resounding "no" from them in response to the question that is titling this hearing, "Has the Department of Homeland Security abandoned the resiliency-based approach?"

This is not about abandoning a resiliency-based approach. The Department fully embraces the concept of resiliency. It is not about protection versus resiliency. It is about both.

It is about achieving an appropriate balance, Madam Chairwoman, as you said in your opening statement. That is what this is all about, because we understand the incredible necessity of being able to absorb an attack of Mother Nature, of Al Qaeda, or some other emergency, and being able to respond, recover, reconstitute quickly.

But we also feel that, in some cases, some of the more extreme advocates of the resiliency construct dismiss the importance of an upfront prevention and protection piece that absolutely has risk as a critical component so that we can direct our energies and resources appropriately.

We cannot afford to protect everything, but we cannot simply stand by and protect nothing. So we have to do things in advance, and we have to do things after the fact to make sure that we are saving American lives, limiting disruption to the economy, and getting American society back on its feet as quickly as possible. That is what this debate is all about, from my perspective.

Our focus on the Nation's critical infrastructure includes actions to mitigate overall risk to assets, systems, networks, functions, and their interconnecting linkages resulting from any type of hazard, whether it be a terrorist attack, and attack by Mother Nature, or a major safety incident.

This includes actions to deter threats, mitigate vulnerabilities, and minimize consequences. Protection can include, in the scope of a national infrastructure protection plan, a wide range of activities, such as hardening facilities, building resiliency redundancy, incorporating hazard resistance into facility or system or network design, initiating active or passive countermeasures, installing security systems, promoting workforce security programs, and implementing cyber measures, among various other precautions.

There cannot be a one-size-fits-all approach, as some would advocate. Rather, we have devised a national-level approach based on a combination of consideration that reflects an understanding of vulnerabilities, interdependencies, and priorities in this all-hazards context.

We view protection as an overarching risk management strategy that is supported by very important and specific congressional and executive branch authorities that fully acknowledge the concept of resiliency where it offers the best solution to managing a particular set of risk at the facility, system, sector, or enterprise level.

Since the 9/11 attacks, we have made significant efforts to define the scope of work required to establish the processes and mechanisms to secure and mitigate the vulnerability of our infrastructures, ensuring their functionality and resiliency in a post-attack or post-incident mode, as well.

Because the private sector owns and operates most of the Nation's infrastructures, DHS has pursued a framework in which government and the private sector work together with our State and local partners in a common approach to set goals and priorities, identify risks, assign roles and responsibilities, allocate resources, and measure progress across this framework. The concept of resiliency is absolutely critical across this framework.

We also recognize that adopting, however, a one-size-fits-all construct would possibly create a very important imbalance. Specifically, we must make sure that our approach incorporates a resiliency-based response and recovery component, as well as an upfront risk-based, risk-directed prevention and protection component.

The chemical, nuclear and energy sectors are prime examples of the need to balance our concern about infrastructure restoration after an incident, with our ability to prevent the release of dangerous chemical substance in the populated areas in the context of these sectors.

After all, preventing the loss of American lives, innocent lives, must remain our No. 1 goal and concern. Our efforts and accomplishment to date, in partnership with many others, reflect this need for a balanced approach between prevention, protection, and resiliency.

In June 2006, we released the National Infrastructure Protection Plan, again, a balanced approach between resiliency, protection, response and recovery activities, and upfront prevention.

The NIPP addresses the importance of resiliency over 52 times throughout the course of the document, and it is the national unifying framework for understanding and managing risks to our Nation's critical infrastructures.

The 17 critical infrastructure plans that were promulgated about a year ago are the product of 18 months of joint effort by CIKR owners and operators, State and local, tribal and territory officials, and Federal officials to make sure that we get this right.

The diversity of the sectors means that different types of protection activities may be most effective for each. Certain sectors are most likely to embrace resiliency as an overarching approach, given their inherent characteristics, while others may focus on specific types of physical protection or cybersecurity or rapid response, to minimize consequences.

Ma'am, I appear with your staff on multiple occasions various elements of the sector-specific plans. Just to highlight some examples, in banking and finance, resiliency integrated in 48 times, communications sector 55 times, dams 10 times, defense industrial base 14 times, energy 34 times, I.T. 24 times, postal and shipping 23 times, transportation 86 times, water 20 times.

The construct and concept of resiliency, working in partnership with upfront, risk-based protection, prevention is thoroughly engrained, embedded and indoctrinated into all the national-level strategies and plans that we have been working on for the past 3 years.

In addition, I brought a copy of the National Infrastructure Protection Plan appropriately marked with all the resiliency pieces of the puzzle flagged for your staff to look at.

I brought recently, last night issued, while I was flying back from overseas, our national hurricane analysis that really focuses on pre-event, pre-landfall hurricane infrastructure impacts, as well as what we think might happen post-landfall, passed that out to our private-sector counterparts.

We recently promulgated the critical infrastructure, resiliency, protection, security, information sharing annex to the national response framework that we will use to guide ourselves and the Nation through hurricane season, as well as a terrorist attack.

Finally, pandemic influenza across the 17 critical infrastructure sectors, in a guide that we built with the private sector, to highlight the need to focus on this type of pestilence from a resiliency perspective.

So I believe that the documents alone at the national level speak to the effort that we have put in to making sure we get this right and to achieve the balance that you spoke to at the beginning of the conversation.

Ma'am, those are my opening remarks. We look very much forward to the discussion and the dialogue with you today and, again, appreciate your collective leadership on this issue.

[The statement of Colonel Stephan follows:]

PREPARED STATEMENT OF ROBERT B. STEPHAN

MAY 14, 2007

Thank you, Chairwoman Jackson Lee, Ranking Member Lungren, and all of the distinguished members of the subcommittee. I appreciate the opportunity to address

you on the role of the Office of Infrastructure Protection (IP) and our many partners, including the private sector, in securing and enhancing the resiliency of the Nation's critical infrastructure and key resources (CIKR). I know you have heard from my counterparts within the Department of Homeland Security on this topic, and I trust you have also received from them a resounding "No" in response to the question titling this hearing, "Has the Department of Homeland Security Abandoned the Resilience-Based Approach?" Since we have been in the process of adjusting to a major change in the American way of life since September 11, 2001, I think it is fair to say that there is resilience built into practically everything that the Department of Homeland Security (DHS) does. In fact, DHS defines resilience as "the ability to recover from, or adjust to, adversity or change." I would like to focus today on how IP works with its partners to ensure that a comprehensive, multifaceted framework exists to support the partnership dedicated to securing and enhancing the resiliency of the Nation's CIKR.

I believe that a recent article in the publication Foreign Affairs provides a good explanation of what we mean by "resiliency." The article stated that there are four factors, that when committed to in a sustained manner, result in resilience.[1] The first is robustness, the ability to keep operating or stay standing in the face of disaster. Second is resourcefulness, which involves skillfully managing a disaster once it unfolds. Third is rapid recovery, defined as the capacity to get things back to normal as quickly as possible after a disaster. Fourth is the statement that resilience means having the ability to absorb the new lessons that can be drawn from a catastrophe. Again, I think that DHS' efforts to date reflect these tenets, and, particularly for the CIKR protection mission, a sustained commitment is an absolute requirement of all members of the partnership.

The CIKR protection mission includes actions to mitigate the overall risk to assets, systems, networks, functions, or their interconnecting links resulting from exposure, injury, destruction, incapacitation, or exploitation. In the context of the National Infrastructure Protection Plan (NIPP), this includes actions to deter the threat, mitigate vulnerabilities, or minimize consequences associated with a terrorist attack or other incident. Protection can include a wide range of activities, such as hardening facilities, building resiliency and redundancy, incorporating hazard resistance into the design of a facility, initiating active or passive countermeasures, installing security systems, promoting workforce surety programs, and implementing cyber security measures, among various others. There cannot be a one-size-fits-all approach to CIKR protection, and we have to devise a strategy based on a combination of considerations that reflects an understanding of vulnerabilities, interdependencies, and priorities in an all-hazards context. We view protection as an overarching risk-management strategy that fully acknowledges and supports the concept of resiliency where it offers the best solution to managing a particular risk or set of risks.

Since 9/11, significant efforts have been underway to define the scope of work required to establish the processes and mechanisms to secure and mitigate the vulnerability and ensure the functionality of CIKR across our country. The private sector has made substantial investments to boost resiliency, increase redundancy, and develop contingency plans. To support these efforts, the Department has provided nearly $14.8 billion in risk-based grant funding—with another $2.5 billion to be distributed this year—to deter threats, reduce vulnerabilities, and build resiliency.

Because the private sector owns and operates most of the Nation's critical infrastructure, DHS has successfully pursued a voluntary partnership approach, where government and the private sector work together under a common framework to set goals and priorities, identify key assets, assign roles and responsibilities, allocate resources, and measure our progress against national priorities. As important as resiliency is to a number of our critical sectors, we recognize that adopting a "one-size-fits-all" solution could create an imbalance. The chemical, nuclear and energy sectors are prime examples of the need to balance our concerns about infrastructure restoration after an incident, with our ability to prevent the release of dangerous substances into populated areas. Preventing the loss of human life must remain our No. 1 goal. Our efforts and accomplishments to date in partnership reflect this need for a balanced approach.

In June 2006, DHS released the NIPP, the overarching goal of which is to "Build a safer, more secure, and more resilient America by enhancing protection of the Nation's CIKR to prevent, deter, neutralize, or mitigate the effects of deliberate efforts by terrorists to destroy, incapacitate, or exploit them; and to strengthen national preparedness, timely response, and rapid recovery in the event of an attack, natural disaster, or other emergency." The NIPP, which uses the word "resiliency" or a vari-

[1] "America the Resilient," Stephen E. Flynn, *Foreign Affairs*, March/April 2008.

ant of it over 50 times, is the national unifying framework for understanding and managing the risk to the Nation's infrastructure through the creation of partnerships with the private sector. The 17 CI/KR Sector Specific Plans (SSPs) required under the NIPP were issued on May 21, 2007. They are the product of almost 18 months of joint effort by the CI/KR owners and operators; State, local, territorial and tribal governments; and the Federal Government to identify and address sector specific risks and implement tailored risk strategies, to include tailored resiliency components.

Specifically, the NIPP provides the coordinated approach to establish national CIKR priorities, goals, and requirements so that Federal funding and resources are applied in the most effective manner to reduce vulnerabilities, deter threats, and minimize the consequences of terrorist attacks, natural disasters, and other incidents. It provides an integrated, risk-based approach to focus Federal grant assistance to State, local, and tribal entities, and to complement relevant private sector activities. It clearly identifies roles and responsibilities of all partners, and includes mechanisms to involve private sector partners in the planning process and supports collaboration among security partners to establish priorities, define requirements, share information, and maximize the use of finite resources. The NIPP serves as the unifying framework to ensure that CIKR investments are coordinated and address the highest priorities, based on risk, to achieve the homeland security mission and ensure continuity of the essential infrastructure and services that support the American government, economy, and way of life.

Achieving the NIPP goals requires meeting a series of objectives that include understanding and sharing information about terrorist threats and other hazards, building security partnerships, implementing a long-term risk management program, and maximizing the efficient use of resources. IP focuses on programs, projects, and activities that are aligned with the NIPP's objectives of Identification and Analysis, Coordination and Information Sharing, and Risk Mitigation Activities. This framework and its goals are foundational to what IP does. Every day, we work with State, local, tribal and territorial leaders and with private sector owners and operators to pursue a common goal of securing the Nation's CIKR against terrorist attacks, natural disasters and other emergencies.

The NIPP provides a Sector Partnership Model through which such coordinated planning and program implementation can take place. The SSPs, developed under the umbrella of this Partnership, reflect the entire range of activities intended to accomplish the goal of security and resiliency for the sectors, and by doing so, increased preparedness. While this may sound like a relatively basic undertaking, it represents probably the first time that the government and the private sector have come together on such a large scale—literally, across every major sector of our economy—to develop a joint plan for how to protect and prepare our CIKR for natural and terrorist-related incidents. The SSPs define roles and responsibilities within each sector, catalog existing security authorities, institutionalize security partnerships already in place; and set clear goals and objectives to reduce risk, much of which also helps to prepare for disasters and set the stage for a resilient approach.

The diversity of the CIKR sectors means that different types of protection activities may be most effective for each. Certain sectors are most likely to embrace resiliency given their inherent characteristics, while others may focus more on specific types of physical protection or training or rapid response to minimize consequences; most represent a combination of various approaches. Some examples of activities focusing on resiliency include:

- In May of each year, the National Infrastructure Coordinating Center (NICC), the 24×7 watch center for coordination and communication with the CIKR sectors, disseminates a series of documents to the CIKR sectors, which includes scenario-driven hurricane impact analyses prepared by the National Infrastructure Simulation and Analysis Center (NISAC).
  - This year, NISAC has prepared 10 separate scenario analyses for simulated hurricanes making landfall in regions at high risk based on historic hurricane activity, population, and potential CIKR impacts. These pre-season analyses are intended to assist the CIKR sectors with enhanced situational awareness and response and recovery planning, based upon simulated impacts to each CIKR sector in those geographical areas, as well as a better understanding of cross sector interdependencies.
- Currently, 24 States have active Water/Wastewater Agency Response Networks (WARN) organizations, with eight more scheduled to develop WARN organizations by the end of the third quarter of 2008. The WARN system development is a direct result of the sectors third goal from the SSP "Maintain a Resilient Infrastructure."

- The Communications SSA, the National Communications System (NCS), participates in various programs that are aimed at building awareness or educating a greater community about the problem of critical infrastructure assurance and resiliency.
  - An example, the Route Diversity Forum periodically helps educate NCS member departments and agencies about improving communications resiliency.
  - To reach out to the broadcast industry, NCS works through the Federal Communications Commission (FCC), trade associations, and the FCC's Media Security and Reliability Council, which is developing best practices to ensure optimal reliability, robustness, and security of broadcast facilities. The NCS also is reaching out to other sectors with which it shares interdependencies and is assisting them in reviewing how their plans address communications interdependencies.
- As part of the Nation's electricity supply infrastructure, the nuclear sector works with regulators and other security partners to ensure that full operations are resumed as safely and quickly as possible following an incident which requires a supply reduction. Furthermore, the sector is working with its security partners to address medical radioisotope supply resiliency in the event of a disruption in the radioisotope supply chain.
  - Under the auspices of its SCC, the Nuclear Sector has completed a pilot of its proposed Prompt Notification program. The Prompt Notification capability will prepare the sector and nearby CIKR assets to defend against a geographically coordinated terrorist attack by providing a real-time mechanism for emergency communications to the Nuclear Sector, Federal entities, and critical infrastructure community partners in the vicinity of a security incident. This program will provide immediate situational and operational awareness in the event of an incident, and to enable more effective response and system restoration.
- The Commercial Facilities Sector represents one of our most diverse sectors. Yet, under the NIPP, it has come together through its SCC, in recognition of its shared risk and shared interest in protecting its assets. The participation within its council shows that there is a strong business case to be made for making investments of this kind. The companies and facilities that take steps to protect assets and plan for emergencies are often the ones that can more quickly recover from a disruption. Joint activities for this sector include:
  - The Commercial Facilities Sector Specific Agency collaboration with the Meridian Institute during their development of the Southeast Region Research Initiative), which includes the Community & Regional Resilience Initiative. These initiatives are intended to develop the processes and tools needed for communities and regions to achieve their highest measurable levels of resilience against disruptions resulting from natural and man-made disasters. Focus is placed on the ability to quickly return citizens to work, reopen schools and businesses, and restore the essential services needed for a full and swift economic and social recovery. Selected cities in the Southeast Region are participating in these initiatives. The ultimate goal of this effort is to strengthen the capability to withstand, prevent, and protect against significant multi-hazard threats so that a community, State, and region, and its private sector partners, can rapidly restore critical services, re-establish the area's economic base, and return to "normal" as quickly and effectively as possible.
  - DHS conducting site assistance visits that incorporated industry feedback into a set of educational reports that owners and operators can use to identify vulnerabilities.
  - DHS providing security training as well as courses on increasing terrorism awareness around commercial facilities. To date, DHS has provided a total of 408 courses for the private sector.
  - Joint participation in major exercises covering terrorism, hurricane preparedness, and pandemic planning.
  - Joint working group between DHS and the National Association for Stock Car Auto Racing (NASCAR) produced a planning guide for mass evacuation and a template for NASCAR facilities to use in coordinating with State and local stake holders and planning. The partnership at each of these sessions included private sector, State, local, Federal partners.
- The Chemical Sector has numerous programs and initiatives which increase the Sector's resiliency. In particular the Sector's dedication to exercises enables the preparation necessary for a real incident.
  - The Chemical Sector has participated in numerous national-level exercises including Top Officials (TOPOFF) and National Level Exercise 2–08 (NLE 2–

08). The Chemical Sector was active in the Cyberstorm II exercise with a dozen private sector participants. Exercises like Cyber Storm II build not only response capability, but also strong organizational and individual connections that help ensure the prevention and mitigation of attacks against our critical systems and networks.

- Developed the Pandemic Flu Guideline for the Chemical Sector—This Annex to the Pandemic Influenza Preparedness, Response, and Recovery Guide for Critical Infrastructure and Key Resources will assist the Chemical Sector plan for a severe pandemic.

- The Dams SSA is participating in the development of a pilot study on regional disaster resilience and risk mitigation for the Columbia River Basin. This effort is conducted in collaboration with the Pacific Northwest Economic Region (PNWER), which leads the coordination efforts. The focus of the pilot is on interdependencies and the cascading impacts associated with disruptions of dams, locks, and levees along the Columbia River Basin. In the event of natural disasters, man-made events, aging infrastructures, and sub-standard conditions, failure of these key assets could affect maritime transportation, energy, agriculture, manufacturing, the overall economy, health and human safety, and national security. The goal of this multi-year effort is to identify a holistic approach with States, localities and relevant key public and private stakeholders.

As per the National Response Framework, the Office of Infrastructure Protection has also instituted the Infrastructure Liaison (IL) to provide the private sector a vital resource during disasters, in part by enhancing the communications that are so vital to resilient systems and sectors. The IL acts as the principal advisor to the Joint Field Office Coordination Group regarding all national and regional CI/KR incident-related issues and assists the Principal Federal Official in the prioritization of protection and restoration efforts. The IL coordinates CI/KR-related issues and actions with the appropriate Emergency Support Functions (ESFs) and other State and local components represented in the JFO, providing valuable reach-back to DHS headquarters and the operational components of the National Operations Center (NOC), including the NOC Watch, the NICC, and the National Response Coordination Center (NRCC). Additionally, the IL provides impacted private sector partners with an established mechanism and process to address requests for information and assistance, either directly or via the NICC, in compliance with applicable policies and laws.

Finally, the CIKR sectors just completed participation in National Level Exercise (NLE) 2–08, which involved both a hurricane making landfall and a chemical terrorism threat. The exercise provided the opportunity for all participants to assess where they have or need redundancy for business continuity, and the ability to deal with significant potential power outages and distribution systems disruptions.

Additionally, we focus on CIKR with the activities of the Homeland Infrastructure Threat and Risk Analysis Center (HITRAC), a joint infrastructure-intelligence fusion center with the Office of Intelligence and Analysis (OI&A). HITRAC analyzes and monitors risks to U.S. CIKR, allowing IP to provide DHS decisionmakers, the Federal CIKR community, owners and operators of CIKR, as well as State, local, and tribal and territorial authorities with actionable analysis and recommendations to manage risk. Analytical products are developed at the asset, sector, region, and national level and provide an understanding of the threat, CIKR vulnerabilities, the potential consequences of an attack, and the effects of risk-mitigation actions.

Again, protection can include a wide range of activities. There cannot be a one-size-fits-all approach to CIKR protection, and we work with a variety of partners in a dynamic risk landscape to prioritize activities and devise a strategy based on a combination of considerations that reflect an understanding of vulnerabilities and interdependencies in the all hazards context. We view protection as an overarching risk management strategy that fully acknowledges and supports the concept of resiliency where it offers the best solution to managing a particular risk or set of risks. The NIPP and its supporting SSPs chart the path forward for continuous improvement of security and resiliency of our critical infrastructures, and the focused activities of IP in concert with all of our CIKR partners ensures their preparedness.

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 Assistant Secretary. Without objection, we will put his entire testimony, including his documents, in the record.

Thank you again. I now recognize Mr. Czerwinski to summarize his statement for 5 minutes.

Welcome.

STATEMENT OF JONAH J. CZERWINSKI, SENIOR FELLOW, HOMELAND SECURITY, IBM GLOBAL LEADERSHIP INITIATIVE

Mr. CZERWINSKI. Given the unique risks of 21st century, resiliency is a necessary goal. The balance you spoke of is key.

I am a senior fellow at IBM's Global Leadership Initiative, where I work on public-sector homeland security challenges from a private-sector perspective, much of it on resilience. For the past 15 months, I have worked on a framework for strengthening commerce, security and resiliency.

Today, I would like to touch upon three things. First, resilience and its definition, which can be an elusive concept, meaning different things to different stakeholders; second, the unique role served by the private sector; and, third, a recommendation for how DHS can engage the private sector in making this a more resilient Nation.

Chairman Thompson said that we all have a role to play, because resilience is the responsibility of the Federal Government, States and localities, academia, and the private sector.

The first step toward accomplishing this is establishing an agreed-upon vision for how we as a Nation can become more resilient. That vision rests upon a clear understanding of what is meant by resilience.

Resilience is the ability to reduce the risk and impact of a terrorist attack or disruption, while also improving the facilitation of trade and travel. In the context of natural disasters, resilience enables people closest to the crisis to act, provides them with the authorities and information necessary to succeed, and employs an effective governance framework.

However, redundancy is not resiliency. Having costly back-up systems or two of everything is the easy, yet most expensive way for infrastructure to bend and not break.

Finally, the private sector is an asset first and a vulnerability second. It is an asset because the goods, people, conveyances and information that comprise private-sector activity interact at critical nodes that must be both protected and viewed as a source of resilience.

This is a critical step toward being able to make the case for private-sector engagement and to establish the form of partnership this committee rightly calls out as a priority.

At IBM, we have been working on the issue of resilience in the global trade system for the past several years. We found that the global trade system can be organized and viewed as a circulatory system of goods, people, conveyances, money and information.

While many things that move through our systems of transportation, immigration and trade are monitored a lot, isn't monitored at all, even fewer things are monitored in conjunction with one another. Yet it is those linkages that often give us the clearest picture of what is going on and what might be going wrong.

A robust framework that embraces the fundamental complexity and networked nature of these systems will identify critical interrelationships, inefficiencies, and vulnerabilities across the flows.

Staying within the stovepiped systems puts our competitiveness and possibly our security at risk.

IBM recently released our paper, entitled "Global Movement Management: Commerce, Security, and Resilience in Today's Networked World," in which my co-authors and I outline an analytical framework we developed to strengthen the global trade system by helping to identify and address vulnerabilities in and across the elements that make up our global movement system. It brings those interrelationships into focus.

This framework requires a partnership between the government and the private sector, because it involves an integrated and evolving mix of preemptive, preventive, preparatory and responsive measures across three vital areas: human capital, technology, and governance.

Individuals within companies and governments face increasingly complex choices about how to perform and address—how to improve performance and address risk.

Strategic human capital requires leaders to employ emerging techniques for managing in a networked environment, some of which are highlighted in my written statement.

We also need to change how we use technology to seek efficiencies. By sharing greater volumes of information, companies and governments can take advantage of open-source techniques to drive innovation and help make the global systems more efficient, resilient and secure.

Governance in this context requires that participants in the global movement systems embrace a more comprehensive set of factors to understand and a means by which to organize their efforts to address the actual risks, costs and benefits that accrue to an organization in today's networked environment.

Our research shows that organizations have successfully met the challenges of organizing efforts across national boundaries, but not yet across sectors.

In summary, to create a system in which security improvements and performance improvements are not mutually exclusive, but mutually reinforcing requires a partnership between the owners and operators of this movement system and the Federal homeland security enterprise.

For this reason, today's hearing represents a productive step forward. With a common vision, better information, with the right technology and well-trained government and commercial employees who are empowered to take action, a more resilient Nation is within reach.

Thank you very much for having me. I look forward to your questions.

[The statement of Mr. Czerwinski follows:]

PREPARED STATEMENT OF JONAH J. CZERWINSKI

MAY 14, 2008

Chairwoman Jackson Lee, Ranking Member Lungren, distinguished Members of the subcommittee, I am pleased to appear before you today. I commend you on your leadership to focus on a resilience-based approach to securing the homeland. Given the unique risks of the 21st century, resilience is a necessary goal.

I am a Senior Fellow with IBM's Global Leadership Initiative where I work on public sector homeland security challenges from a private sector perspective, much

of it on resilience. I am also Managing Consultant for IBM's Global Business Services practice. For the past 15 months I have worked on a framework for strengthening commerce, security, and resiliency.

Today, I thought it would be useful to focus on three things.

- First, really defining resilience, which can be an elusive concept meaning different things to different stakeholders;
- Second, the unique role served by the private sector; and
- Third, a recommendation for how DHS can better engage the private sector in making this a more resilient Nation.

Chairman Thompson said that "we all have a role to play" because resilience is the responsibility of the Federal Government, States and localities, academia, and the private sector.

The first step toward accomplishing this is establishing an agreed upon vision for how we as a Nation can become more resilient. That vision rests upon a clear understanding of what is meant by resilience.

I. DEFINING RESILIENCE

Resilience is the ability to reduce the risk and impact of a terrorist attack or disruption while also improving the facilitation of trade and travel. In the context of natural disasters, resilience enables people closest to the crisis to act, provides them with the authorities and information necessary to succeed, and employs an effective governance framework.

Resilience helps to avoid unintended consequences: Resilience—if done right—affords the decisionmaker the enhanced ability to focus response efforts on the part of the system that is actually stressed and limits the risk of over-reacting, which often times leads to unintended consequences.

Many suggest that resilience is the ability to "bounce back." And it is, but resilience is different from response and recovery.

Redundancy is not resiliency. Having costly back-up systems or two of everything is the easy yet most expensive way for infrastructure to "bend and not break." If done correctly, resiliency is more akin to the concept of Intelligent Immunity that we put forth in the most recent IBM report on Global Movement Management, and which I'll touch upon in a moment.

II. UNIQUE ROLE OF THE PRIVATE SECTOR

Finally, the private sector is an asset first, and a vulnerability second: It is an asset because the goods, people, conveyances, and information that comprise private sector activity interact at critical nodes that must be both protected and viewed as a source of resilience. This is a critical step toward being able to make the case for private sector engagement and to establish the form of partnership this committee rightly calls out as a priority.

At IBM we have been working on the issue of resilience in the global trade system for the past several years. We found that the global trade system can be organized and viewed as a circulatory system of goods, people, conveyances, money, and information.

While many things that move through our system of commerce are monitored to a greater or lesser extent, a lot isn't monitored at all. Even fewer things are monitored in conjunction with one another.

And yet it is those linkages that often give us the clearest picture of what's going on and what might be going wrong.

A robust framework that embraces the fundamental complexity and networked nature of these systems will identify critical interrelationships, inefficiencies, and vulnerabilities across the flows. Staying within a stovepiped system puts our competitiveness and possibly our security at risk.

III. A FRAMEWORK TO SUPPORT DHS LEADERSHIP IN BUILDING A RESILIENT NATION

IBM recently released our paper entitled "Global Movement Management: Commerce, Security, and Resilience in Today's Networked World," in which my coauthors and I outline an analytical framework we developed to strengthen the global trade system by helping to identify and address vulnerabilities in and across the elements that make up our global movement system. It brings the interrelationships into focus.

This framework requires a partnership between the government and the private sector because it involves an integrated and evolving mix of preemptive, preventive, preparatory and responsive measures across three vital areas: Human Capital, Technology, and Governance.

Strategic Human Capital

Individuals within companies and governments face increasingly complex choices about how to improve performance and address risk. Individual managers and employees face unprecedented volumes of information, new technologies and competitive pressures that complicate their work. At the same time, in a networked economy, decisions made at the individual level can have increasingly global ramifications. Strategic human capital requires leaders to employ emerging techniques for managing in a networked environment. These techniques include improved collaboration, latitude to reach across and outside organizational boundaries, investment in organizational transformation, enhanced technology and, above all, greatly improved training.

Technology

We need to change how we use technology to simplify work processes and seek efficiencies. By sharing greater volumes of information, companies and governments can take advantage of open-source techniques to drive innovation and help make global systems more efficient, resilient, and secure. Upstream companies can be better equipped to provide warnings of supply shortages or other disruptions before they affect downstream partners. Downstream companies can provide early warnings about demand or delivery disruptions to those upstream. Governments can augment counterterrorism efforts with more accessible commercial data while also providing a higher degree of protection for privacy and civil liberties than is currently the case.

Governance

Governance in this context can be characterized by the lack of a coordinated approach that is necessary to address networked risk. Call this a "governance gap." To bridge this gap, participants in the global movement systems need to embrace a more comprehensive set of factors to understand the actual risks, costs, and benefits that accrue to an organization in a networked environment. Moreover, participants need a means by which to organize their efforts to address these risks, costs, and benefits. Our research shows that organizations have successfully met the challenges of organizing efforts across national boundaries but not yet across sectors.

CONCLUSION

In summary, to create a system in which security improvements and performance improvements are not mutually exclusive, but mutually reinforcing, requires a partnership between the owners and operators of this global movement system and the Federal homeland security enterprise. For this reason, today's hearing represents a productive step forward.

With a common vision, better information, with the right technology and well-trained government and commercial employees who are empowered to take action—a more resilient nation is within reach.

Thank you.

Ms. JACKSON LEE. We thank you for your testimony.

I now recognize Mr. Johnson to summarize his statement for 5 minutes.

STATEMENT OF SHAWN JOHNSON, VICE CHAIRMAN, FINANCIAL SERVICES, SECTOR COORDINATING COUNCIL

Mr. JOHNSON. Thank you. Thank you, Chairwoman Jackson Lee, Ranking Member Lungren, and members of the committee.

I am Shawn Johnson, chairman of the Investment Committee for State Street Global Advisors and vice chairman of the Financial Services Sector Coordinating Council, or FSSCC, a volunteer position.

My comments today focus on efforts to improve resilience in the financial services sector, and in particular the resilience-based related activities of the FSSCC.

Thought established at the request of the Department of Treasury, the FSSCC is a private-sector coalition working to improve the

financial sector's resilience to terrorist attacks, manmade and natural disasters, cyber attacks, and other threats.

In general, the U.S. financial services sector has performed well in times of crisis. While events such as 9/11 and the attacks have revealed some weaknesses in the resilience of our financial systems, industry and government have responded and work cooperatively to address these weaknesses.

Some of the government's resilience activities have been in the form of specific regulatory proposals, such as the issuance of the best practices white paper by the Federal Reserve, the OCC, and the SEC in 2003, addressing contingency planning and backup facilities for clearing and settlement activities.

Implementation of the white paper has required significant changes in business practices and substantial investment by financial investment firms. But the result has been a more resilient financial services system.

The government participates in other, less formal activities, such as working with local public-private partnerships to sponsor resilience exercises, which simulate flu pandemic, natural disasters, or other terrorist events, and provide valuable lessons to both the public and the private sector.

Much of the work of FSSCC, of which I am currently vice chair, has focused on resilience.

For example, the FSSCC has been working to improve industry access to emergency credentials, which are critical in times of emergency. We have also worked to expand the GETS program, which provides access to priority telephone services during a crisis.

We held a cybersecurity summit in February 2008 with private- and public-sector participation, and the FSSCC and FBIIC have since each launched new cybersecurity committees.

The FSSCC maintains relationships to help align academic research with real-world business needs and offers programs such as the FSSCC SMART program, which provides subject matter expertise from financial institutions to R&D organizations.

The FSSCC is an active participant in the Partnership for Critical Infrastructure Security, which is dedicated to coordinating cross-sector initiatives.

Our infectious disease forum develops and communicates information and strategies the private sector can employ to prepare for an avian flu pandemic or other infectious disease outbreak. In addition, all FSSCC members are active with their own resiliency efforts aimed at their particular segment of the financial services industry.

These efforts are summarized in the FSSCC's annual report, which can be found on the FSSCC Web site.

I would like to conclude my testimony today by describing one of the largest financial services industry resilience exercises to date, the FBIIC–FSSCC Pandemic Flu Exercise of 2007.

The exercise was a public-private partnership, sponsored by the FBIIC, the FSSCC, and SIFMA. It was conducted in the fall of 2007 and simulated a pandemic flu impacting the financial services sector.

More than 2,700 financial services organizations participated. Participation was voluntary, free of cost, and open to all organizations within the U.S. financial services sector.

The results were aggregated, with anonymity provided by the participating institutions. Participants were given scenarios to implement that represented an escalating pandemic flu epidemic. At the height of the exercise, for example, absentee rates in some cases reached 49 percent, a level sufficient to stress even the best contingency planning efforts.

The performance of the financial services sector under the conditions simulated by the exercise was laudable, but not perfect. In general, it appeared that, while there would have been significant impacts to the financial sector, it would have continued to cope and operate.

Perhaps more important than the immediate results of the exercise, however, is the reaction of the participants: 99 percent of participants found the exercise useful in assessing their organization's business-planning needs; 97 percent of participants said the exercise allowed their organization to identify critical dependencies, gaps, and seams that warrant additional attention; and 91 percent said their organization planned to initiate additional all-hazard plan refinements.

Full details of the exercise are provided in the after action report.

Overall, I think the pandemic exercise provides a good example of the potential benefit of the strong public-private partnership that exists. While continuity and resilience planning are certainly key regulatory and enforcement issues, it is clear to me, as a representative from the private sector, that the quality of the data obtained was considerably improved by the cooperative and anonymous nature of the exercise.

As a result, both the private and public sectors were able to obtain insights that would have been difficult or impossible to obtain through standard regulatory channels.

Once again, thank you for providing me the opportunity to testify on behalf of the FSSCC. I will be pleased to answer any questions you have.

[The statement of Mr. Johnson follows:]

PREPARED STATEMENT OF SHAWN JOHNSON

MAY 14, 2008

Chairwoman Jackson Lee, Ranking Member Lungren, and members of the Subcommittee on Transportation Security and Infrastructure, I am Shawn Johnson, Chairman of the Investment Committee of State Street Global Advisors and Vice-Chairman of the Financial Services Sector Coordinating Council (FSSCC). I am pleased to submit this testimony today on behalf of the FSSCC.

I appreciate the subcommittee's invitation to testify at this hearing, titled "Partnering with the Private Sector to Secure Critical Infrastructure: Has the Department of Homeland Security Abandoned the Resilience-Based Approach?" Given my position with the FSSCC, my comments today focus on the experience of the financial services sector with regard to resilience, and, in particular, resilience related activities in which FSSCC has participated.

The FSSCC was established at the request of the U.S. Department of the Treasury in 2002 in response to Homeland Security Presidential Directive 7, which required sector-specific Federal department and agencies to identify, prioritize, and protect United States critical infrastructure and key resources. We are a private sector coalition of financial services firms and trade associations working to reinforce

the financial sector's resilience to terrorist attacks, man-made and natural disasters, cyber attacks, and other threats to the sector's critical infrastructure.

The FSSCC closely interacts with its Sector Specific Agency (SSA), the Department of the Treasury, it public-sector counterpart, the Financial and Banking Information Infrastructure Committee (FBIIC), and the Department of Homeland Security. Membership lists for the FSSCC and the FBIIC are attached.

We also strongly support regional public/private partnerships, such as ChicagoFIRST, DFWfirst, and numerous others. These organizations address homeland security and emergency management issues at the local level, where many catastrophic events are primarily managed.

In general, the U.S. financial services sector has performed well in times of crisis. While events such as the 9/11 attacks have revealed some weaknesses in the resilience of our financial systems, industry and government have responded, and worked cooperatively to address these weaknesses.

Some of the government's resilience activities have been in the form of specific regulatory proposals, such as the issuance of the Interagency White Paper on Sound Practices to Strengthen the Resilience of the U.S. Financial System in 2003 by the Federal Reserve, OCC and SEC.

The White Paper addressed the importance of resilience in financial clearing and settlement activities critical to U.S. financial markets, and is intended to reduce systemic risk created when primary and back-up facilities and staffs are located within the same geographic region. Implementing the requirements of the White Paper has required significant changes in business practices, and substantial investment, by financial services firms—but the result has been a more resilient U.S. financial system.

Formal rulemaking, however, is not the government's only means of improving the resiliency of our financial infrastructure. For example, the Department of the Treasury has worked with local public/private partnerships to sponsor several resilience exercises, including:

- A pandemic exercise in Chicago in December, 2006 (with ChicagoFIRST),
- A pandemic exercise in San Francisco in May, 2007 (with BARCfirst),
- A radiological attack exercise in Tampa Bay in July, 2007 (with FloridaFIRST), and
- A hurricane exercise in Alabama in March, 2008 (with Alabama Recovery Coalition for the Financial Sector).

Other similar exercises are being planned, including a terrorist attack simulation involving all of the regional coalitions (through RPC FIRST) in San Francisco this week.

Much of the work of the FSSCC, of which I am currently Vice-Chairman, has also focused on resilience. FSSCC resilience-related activities include:

- *Emergency Credentialing*.—The ability of the private sector to obtain security credentials during times of emergency is a critical element to the financial services sector's resiliency. The FSSCC has been involved in efforts to encourage States to adopt credentialing programs, and expansion of the GETS program. The GETS Program allows critical infrastructure operators to gain priority telephone service during a crisis.
- *Cyber Security*.—A Cyber Security Summit was held in February, 2008 with information technology leaders from across the public and private sectors, to discuss threats to the financial sector from cyber vectors. The FSSCC and FBIIC have since each launched new cyber security committees, whose mission is to work with the financial services sector to strengthen cyber security and resilience of current and future IT operations.
- *Research and Development*.—The FSSCC and its R&D Committee encourage alignment of research into infrastructure protection through outreach to academic institutions, and programs such as FSSCC SMART, which provides subject matter expertise from financial institutions to research and development organizations.
- *Cross-Sector Cooperation*.—FSSCC is an active participant in the Partnership for Critical Infrastructure Security (PCIS), which is dedicated to coordinating cross-sector initiatives to improve the security and safety of U.S. financial infrastructure.
- *Infectious Disease Forum*.—A long-standing FSSCC work group is the FSSCC Infectious Disease Forum. The purpose of the Infectious Disease Forum is to develop and communicate information and strategies that FSSCC members and their member organizations may employ to prepare for an avian flu pandemic or other infectious disease outbreak.

These ongoing efforts, and others, demonstrate the FSSCC's strong commitment to resiliency. In addition, all FSSCC members are active with their own resiliency

efforts, aimed at their particular segment of the financial services industry segment. These efforts are summarized in FSSCC's annual report, which can be found on the FSSCC Web site *(https://www.fsscc.org/fsscc/reports/2007/annual_report_2007.pdf)*.

I'd like to conclude my testimony today by describing one of the largest financial services industry resilience exercises to date, the FBIIC/FSSCC Pandemic Flu Exercise of 2007.

This exercise, conducted in Fall 2007, simulated a pandemic flu impacting the financial services sector, and was intended to:

- Enhance the understanding of systemic risks to the financial sector;
- Provide an opportunity for firms to examine the effectiveness of their pandemic plans; and
- Explore the effects of a pandemic flu on other crucial infrastructures impacting the financial services sector.

The exercise was a public/private partnership, organized by the FBIIC, the FSSCC, and the Securities Industry and Financial Markets Association (SIFMA), the trade association representing the securities industry.

By all accounts, the execution of the exercise was a success. More than 2,700 financial organizations participated. Participation was voluntary, free of cost, and open to all organizations within the U.S. financial sector. Results were aggregated, with anonymity provided to participating institutions. The exercise was intended to simulate the medical, financial, and societal impacts of a pandemic flu, and gather information about how financial institutions were able to react to such scenarios. At the height of the exercise, for example, absentee rates in some cases reached 49 percent, a level sufficient to stress even the best contingency planning efforts.

The performance of the financial sector under the conditions simulated by the exercise was laudable, but not perfect. In general, it appeared that while there would have been significant impacts to the financial services sector, it would have continued to cope and operate.

Perhaps more important than the immediate results of the exercise, however, is the reaction of the participants:

- 99 percent of participants found the exercise useful in assessing their organizations business planning needs;
- 97 percent of participants said the exercise allowed their organization to identify critical dependencies, gaps, and seams that warrant additional attention; and
- 91 percent said their organization planned to initiated additional all-hazard plan refinements based upon lessons learned during the exercise.

The After Action Report, issued in January 2008, provides considerable detail on the results of the exercise, both in aggregate and by industry segment, as well as numerous illustrations of possible opportunities for further improvement, for both the public and private sector. One such area for improvement is in the area of regulatory relief. Discussions between the private sector and the regulators continue regarding possible regulatory relief during a pandemic. The industry recently started developing an internet-based application to facilitate the collection of information to better gauge the health of the sector.

Overall, the pandemic exercise provides a good example of the potential benefit of strong public/private cooperation and collaboration. While continuity and resilience planning are certainly key regulatory and enforcement issues, it is clear to me as a representative of the private sector that the quality of data obtained was considerably improved by the cooperative, and anonymous, nature of the exercise. As a result, both the private and public sectors were able to obtain insights that would have been difficult or impossible to obtain through standard regulatory channels.

Once again, thank you for providing me the opportunity to testify on behalf of the FSSCC. I would be pleased to answer any questions.

APPENDIX

FSSCC MEMBERS

American Bankers Association; American Council of Life Insurers; American Insurance Association; American Society for Industrial Security (ASIS) International; BAI; BITS/The Financial Services Roundtable; ChicagoFIRST; Chicago Mercantile Exchange; The Clearing House; CLS Group; Consumer Bankers Association; Credit Union National Association; The Depository Trust & Clearing Corporation (DTCC); Fannie Mae; Financial Information Forum; Financial Services Information Sharing and Analysis Center (FS–ISAC); Financial Services Technology Consortium (FSTC); Freddie Mac; Futures Industry Association; ICE Futures U.S.; Independent Commu-

nity Bankers of America; Investment Company Institute; Managed Funds Association; The NASDAQ Stock Market, Inc.; National Armored Car Association; National Association of Federal Credit Unions; National Association of Securities Dealers (NASD); National Futures Association; NACHA—The Electronic Payments Association; The Options Clearing Corporation; Securities Industry Automation Corporation (SIAC); Securities Industry and Financial Markets Association (SIFMA); State Street Global Advisors; VISA USA Inc.

FBIIC MEMBERS

American Council of State Savings Supervisors; Commodity Futures Trading Commission; Conference of State Bank Supervisors; Department of the Treasury; Farm Credit Administration; Federal Deposit Insurance Corp; Federal Housing Finance Board; Federal Reserve Bank of New York; Federal Reserve Board; National Association of Insurance Commissioners; National Association of State Credit Union Supervisors; National Credit Union Administration; North American Securities Administrators Association; Office of the Comptroller of the Currency; Office of Federal Housing Enterprise Oversight; Office of Thrift Supervision; Securities and Exchange Commission; Securities Investor Protection Corporation.

Ms. JACKSON LEE. Mr. Johnson, thank you very much for your testimony.

I now recognize Mr. Raisch to summarize his statement for 5 minutes.

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

Mr. RAISCH. Chairwoman Jackson Lee, Ranking Member Lungren, and distinguished members of the subcommittee, thank you for inviting me this afternoon to testify on the vital issue of private sector resilience and, in particular, the Voluntary Private Sector Preparedness Certification Program called for by the implementing recommendations of the 9/11 Commission Act of 2007.

I am most honored to join you from the International Center for Enterprise Preparedness at New York University. As you mentioned, the center serves as the first academic center focused specifically on private-sector resilience and preparedness.

I am also most honored to have served as a private-sector adviser to the 9/11 Commission.

More importantly, though, I am here to reflect on the perspective garnered from 12 forums on this specific voluntary certification program held since this past fall involving over 550 private-sector representatives and current five different working groups, with over 250 participants in the private sector.

Let me clearly state that there is substantial and growing interest and also concern in the private sector on this program. That being said, also, in preface, I would like to say that it is my personal opinion that this single program has the potential for doing more to institutionalize or economically embed private-sector preparedness than much of the outreach, ad campaigns, and other well-meaning and perhaps productive public affairs efforts to date.

However, this is achievable if and only if two items are addressed in priority. One, it must focus on enabling real economic value to businesses. Further, it must actively and directly involve and engage the private sector in the development and ongoing implementation of the program itself.

Allow me to outline, perhaps, a couple of key considerations for this program going forward and to acknowledge, as well, that much

good work has been accomplished by a variety of organizations in the arena of public-sector preparedness and resilience.

At our center, we have tried to reflect on this and really present you with perhaps some key themes in that respect.

From that, we see four basic themes evolving.

They are, one, firstly and foremost, with respect to this program, we need to assure that voluntary certification in this program is a private-sector-led effort, that it specifically addresses private-sector needs through the ongoing engagement of key stakeholders. This engagement must involve both DHS and the ultimate accrediting body to be chosen.

Secondly, it must build on existing efforts, specifically those efforts in certification, standards, and elements of accrediting bodies. These basic building blocks already exist for the program. The program should seek to integrate them and focus them on private-sector preparedness.

There are existing standards that have been developed by the private sector. Further, there are existing accreditation and certification processes that have been utilized in private-sector voluntary certification in such areas as quality management, the ISO 9000 accreditation program, and environmental management, the ISO 14000 program.

These processes were developed with active involvement of the private sector and have evolved with private-sector application for over 2 decades, in many cases.

There is also an existing accrediting body, ANAB, which has administered private-sector certification for years, as well. I am happy to note that this body has been preliminarily designated by DHS as the appropriate body for the program itself.

Thirdly, the program should allow for flexibility, potentially utilizing a high-level umbrella or framework approach that can be used independently to relate multiple focused standards and practices, which business may already be using.

Key organizations in the private sector have already developed a seminal work on this, the framework for preparedness, on a voluntary basis, sponsored by the Alfred P. Sloan Foundation.

A real effort must be made to recognize, also, and accredit effective activities already in practice by each key sector. These sectors must be brought directly into the process.

Fourthly and finally, that we must enable potential market-based incentives through the involvement of their stakeholders and needs. First and foremost, business practitioners must be actively involved in the development of this program to assure that the program has real operational value.

Secondly and as importantly, potential incentive stakeholders should be directly involved in the process, including supply chain management community representatives, legal counsel, insurance companies, rating agencies, and other reporting entities.

Key action items for government are an opportunity in this respect. I would suggest they are as follows, and I would preface it by the fact that I would underline government in this case can truly be a catalyst, it can be a convener, and it can be, if you will, an investor, at least from a seed-funding perspective on this important process.

Firstly, both DHS and ultimately the accrediting body it designates must actively and consistently engage the private sector in the development implementation of the program. Specific considerations and issues are identified in my written remarks in this respect.

DHS must also continue to maintain its integrated approach to supporting this program, which includes FEMA currently as program lead, but also active involvement by infrastructure protection, science and technology, and the DHS private-sector office, as well as others, as appropriate.

Additionally, other agencies in the executive branch, including Commerce and SBA, should have involvement.

Congress should provide the resources, also, to enable ongoing commitment by DHS to this program. It is an investment that will yield substantial benefits, in terms of societal resilience, given the role the private sector plays in backbone critical infrastructure and dramatic impacts on the overall economy.

Additionally, DHS should continue to evaluate the overall opportunity for voluntary participation in the program by the critical infrastructure business sectors. This community can bring much insight to the program and may find significant value in the assessment capability of the program.

Furthermore, the program may provide a very valuable tool in cross-sector cooperation and assessment. A common reference platform—a Rosetta Stone, of sorts—could aid in sharing best practices and crosspollination across sectors.

Education and tools must also be developed by key stakeholders, optimally with government support, to enable businesses, large and small, to pursue program assessment and implementation with minimal cost and disruption. Key trade and professional associations may be very helpful in this regard.

In addition and finally, Congress should consider enabling incentives for the program, including potentially facilitating effective public reporting and appropriate acknowledgement of proactive companies in this respect.

Additionally, Congress should consider legal liability protections for those proactive firms that undertake certification, perhaps including safe harbors and privilege for vulnerability assessments.

Finally, enabling key industries, such as the insurance industry, to consider industry-wide incentives or initiatives in this regard around the issue of resilience, without concern of antitrust considerations, should also be addressed by Congress.

I welcome your questions. Thank you.

[The statement of Mr. Raisch follows:]

PREPARED STATEMENT OF WILLIAM G. RAISCH

MAY 14, 2008

Chairwoman Jackson Lee, Ranking Member Lungren, and distinguished members of the subcommittee, thank you for inviting me to testify on the vital issue of private sector resiliency and the Voluntary Private Sector Preparedness Certification Program called for by Title IX, Section 524 of Pub. L. 110–523, The Implementing Recommendations of the 9/11 Commission Act of 2007.

As with many undertakings in the private sector, this new program offers both substantial opportunity and significant risk, most especially if the private sector is not effectively engaged. It will be the balancing of these two elements that will de-

termine the ultimate success or failure of this program. It is an effort though that I believe to be well worth undertaking for sake of both the individual businesses and our wider society.

THE 9/11 COMMISSION'S PRIVATE SECTOR RECOMMENDATIONS FOCUSED ON THE "WHAT" AND "WHY" OF PREPAREDNESS

As you may be aware, our Center, the International Center for Enterprise Preparedness (or InterCEP) at New York University is the first academic research center dedicated to private sector resilience. Our activities regularly involve outreach to hundreds of businesses, much of it through interactive forums focused on key issues.

The Center takes its primary focus from the private sector recommendations of the 9/11 Commission, which I was honored to advise on private sector preparedness.

The Commission's recommendations and thus InterCEP's research focus on promoting private sector preparedness through the linking the "what" and the "why" of preparedness/resilience. The 9/11 Commission clearly understood that absent a compelling bottom-line rationale for preparedness, businesses would not invest the funds and other resources necessary to develop a preparedness program. The Commission sought to leverage basic market-based economics, bottom-line orientation, to promote effective private sector preparedness activities by business. They did so with an initial focus on two key elements:

1. Identifying a consensus-based industry standard for business preparedness (the what to do); businesses were looking for a high-level set of criteria that represented best practices in preparedness yet allowed the business flexibility as to how to achieve particular outcomes.
2. Identifying potential incentives for businesses to voluntarily conform with that standard (the why to do it) including mitigating legal liability after an event, potential insurance recognition, and encouraging rating agency acknowledgement (all in addition of course to the basic rationale of continuity of the business in the aftermath of a crisis).

THERE IS A NEED FOR A MEASUREMENT APPROACH/TOOL TO ASSESS BUSINESS PREPAREDNESS

Since establishing our Center in October of 2004 and the extensive research and interface with business that followed, it has become clear that the linkage of the "what" and "why" of preparedness often requires measurement or assessment to determine if the "what" to do of preparedness has been or is being accomplished so that the "why" to do it can be confirmed or rewarded. Thus, there is a third key element that our research with the business sector has identified as critical to successfully promoting private-sector preparedness:

3. A method to measure or assess achievement of preparedness objectives, i.e., identifying "if preparedness is being achieved."

Measurement is important for several reasons. Internally, there are multiple benefits:

- First and foremost, a business needs a yardstick to assess if it is achieving its preparedness goals for which it may have invested effort and resources to assure its business continuity.
- Measurement may also have reputational benefits for corporations that wish to demonstrate to their customers and other stakeholders that they are prepared.
- Measurement may additionally help advance corporate governance goals, especially in validating risk management efforts.

External to the firm, potential "incentives stakeholders" such as supply chain partners, insurance underwriters, rating agencies and the legal community need a credible confirmation that preparedness efforts have been undertaken. These communities generally grant that there is value in preparedness efforts by businesses, and these stakeholders may be disposed toward acknowledging or rewarding preparedness in their activities.

These potential incentives stakeholders do not however wish to undertake the actual assessment or measurement of preparedness on their own on a business-by-business basis. They do not want to nor do they have the resources to send out assessors to a business to ascertain if a particular business's program conforms to a particular industry standard. Yet, if there was a credible program which indicated compliance with such a standard, these stakeholders may consider rewarding it, at least over time. Thus, external benefits to measurement include:

- Measurement could promote resilience of supply chains by supplying a common approach and tool for assessing supplier preparedness.

- A common measurement program may make it easier for various business incentive communities to acknowledge the value of effective preparedness (e.g., insurance, legal, rating agency, etc.) overtime.
- Measurement to a commonly recognized standard may help facilitate exchange of best practices, enabling business to more easily compare practices across industries and sectors which may have distinct terminology and approaches but lack a "rosetta stone" or common set of criteria to compare their efforts.
- A common measurement program may also enable more consistent benchmarking to other firms both within and industry and potentially across sectors—including potentially the critical infrastructure sectors.

THE DEVELOPING VOLUNTARY PRIVATE SECTOR PREPAREDNESS CERTIFICATION PROGRAM

It is in light of these three elements: (1) what to do, (2) why to do it, and (3) a measurement of achievement that I would like to discuss the developing Voluntary Business Preparedness Certification Program.

This new program is proving to be a distinct catalyst, with significant initial and potential impact on private sector preparedness. It is also a program that nonetheless must be guided by key considerations and private sector input to assure its success.

This new program could potentially integrate:

- The "what to do" in the form of one or more preparedness standards to be designated under the legislation,
- An evolving "why to do it" by proactively identifying the business case for preparedness and integrating its elements into the program where possible including potential incentives stakeholders in the process of program development and implementation,
- A credible measurement/assessment methodology based upon historic experience with other voluntary certification programs such as those in quality management (ISO 9000) and environmental management (ISO 14000) which have been implemented in and by the private sector for decades.

The announcement of this program has already to date provided a catalyst for business sector activity. Despite the legislation's annunciation that the program is to be voluntary, the perceived threat of potential government regulation along with other concerns has motivated significant private sector activity. Much of it based on the presumption that the private sector must take the lead in this process to assure that the outcome has positive value and not onerous impact.

For example, one remarkable effort involved four key professional organizations coming together to define the core elements of private sector preparedness based on existing standards and professional practices across multiple disciplines. This effort was sponsored by the Alfred P. Sloan Foundation which is a key funder of InterCEP's activities and involved representatives from ASIS International (a key security association), the Disaster Recovery Institute International (a key business continuity association), the National Fire Protection Association (which maintains the Standard on Disaster/Emergency Management & Business Continuity referenced in the legislation and endorsed by both the 9/11 Commission and DHS) and the Risk & Insurance Management Society (a leading risk management society for businesses). These organizations collectively defined a framework for voluntary preparedness that supports a flexible approach to assessing preparedness potentially including multiple standards reflecting a common core set of preparedness elements. The final report is available at *www.sloan.org*.

Additionally, other organizations have begun forums to discuss the program including the U.S. Chamber of Commerce among others. As an example, InterCEP currently has dozens of businesses actively engaged in five different Working Groups which initially address key potential incentive areas for program acknowledgement:

- Supply chain management;
- Legal liability mitigation;
- Insurance;
- Rating agency acknowledgement;
- Business reporting acknowledgement/crediting.

KEY CONSIDERATIONS AND CONCERNS OF THE PRIVATE SECTOR

Key considerations and concerns identified by the private sector through a diversity of forums hosted by the Center are outlined in the Appendix. The key themes include:

1. Assure that the program is private sector led and addresses private sector needs through ongoing engagement of key stakeholders.
2. Build on the existing including existing standards, proven accreditation/certification processes and established industry practices—key building blocks already exist.
3. Allow for flexibility potentially utilizing a high-level umbrella or framework standard which can be used independently or to relate multiple more focused standards and practices which business may already be using.
4. Enable potential market-based incentives through involvement of their stakeholders and concerns.

ACTION ITEMS FOR GOVERNMENT GOING FORWARD

It will be vital to the ultimate success of the program that government take the initiative as a catalyst and investor in this process:

- Both DHS and the ultimate accrediting body to be designated by it must actively and consistently engage the private sector in the development and implementation of the program. Specific considerations and issues are identified in the Appendix.
- DHS must continue to maintain its integrated approach to supporting this program which includes FEMA as program lead but also includes active involvement by Infrastructure Protection, Science & Technology and the DHS Private Sector Office (and others as appropriate).
- Congress should provide the resources to enable an ongoing commitment by DHS to this program. It is an investment that will yield substantial benefits in terms of societal resilience given the role that the private sector plays in backbone critical infrastructure for our Nation.
- DHS should continue to evaluate the voluntary application of the program to critical infrastructure as this community may find significant value in the capability of the program. Furthermore, the program may provide a very valuable tool in cross-sector cooperation and assessment.
- Education and tools must be developed by key stakeholders (optimally with government support) to enable business (large and small) to pursue program assessment and implementation with minimal cost and disruption.

APPENDIX.—SUMMARY OF INTERCEP RESEARCH TO DATE ON THE VOLUNTARY PRIVATE SECTOR PREPAREDNESS CERTIFICATION PROGRAM

PER TITLE IX, SECTION 524 OF PUB. L. 110–523, THE IMPLEMENTING RECOMMENDATIONS OF THE 9/11 COMMISSION ACT OF 2007

MAY 14, 2008

Key Points & Considerations

Four basic themes are reflected in the following considerations, they are:

1. Assure that the program is private-sector-led and addresses private-sector needs through ongoing engagement of key stakeholders.
2. Build on the existing including existing standards, proven accreditation/certification processes and established industry practices—key building blocks exist.
5. Allow for flexibility potentially utilizing a high-level umbrella or framework standard which can be used independently or to relate multiple more focused standards and practices which business may already be using.
6. Enable potential market-based incentives through involvement of their stakeholders and concerns.

Specific Considerations

- *Early and continuing stakeholder involvement must be maintained to assure that the program is private-sector led.*—While government can play a catalytic role in the early development of the program, ultimately the program should be market-driven as has been the case with the continuing voluntary certification programs in quality and environmental management. Key to assuring that the voluntary certification program has real operational value to business is to involve the full-spectrum of the business sector in the development and ongoing implementation of the voluntary certification program.
- *There is concern within the private sector that the program could develop into a mandatory requirement by government.*—Similar concerns exist about whether the program will be truly voluntary once market pressures force firms to pursue certification in order to remain competitive.

- *There are concerns about the potential costs and liabilities associated with the program*.—It will be important to contain the implementation costs and minimize the bureaucracy associated with the certification process.
- *The program should build on existing voluntary accreditation and certification processes. There are lessons to be learned from historical experience with existing voluntary certification programs in quality and environmental management*.—Current voluntary certification programs in quality management and/or environmental management utilize established processes for accreditation and certification. These could potentially be utilized in the development of the preparedness certification program thereby avoiding significant time and effort as well as benefiting from substantial historical application. Furthermore, opportunities and efficiencies might potentially be achieved by businesses that currently have existing quality and environmental programs by building upon them (i.e., existing management processes). For example, the program should be informed by lessons learned from C–TPAT and pandemic planning regarding the best way to minimize impacts on business and maximize benefits to business.
- *Existing efforts of key vertical industries, such as the financial services sector, should be acknowledged and incorporated into the voluntary certification program*.—Some business sectors have a long history in preparedness activities and robust programs in place. The financial services sector is one. The new law specifically calls for existing industry efforts, standards, practices and reporting in the area of preparedness not be duplicated or displaced but rather recognized and integrated where appropriate. Opportunities should be evaluated with each sector to see not only how their existing efforts can be credited in the process but also how the new certification program can address unique issues important to their sector. Sector coordinating councils and key industry associations should be involved.
- *A "maturity model" or multi-level approach should be considered*.—A "maturity model" approach should be considered which could acknowledge various levels of preparedness and depth of program; for example: Level 1, Level 2, Level 3, etc. This could be helpful in several ways. Depth of program capacity could vary based on how critical a particular organization is in a supply chain. Levels could also be used as targets for progression over the course of time to allow for a step progression from a lower level of preparedness to a higher level. Furthermore, levels may be appropriate in considering expectations for small, medium and large organizations with their varying levels of size, complexity and resources.
- *The voluntary certification should credit/integrate other business reporting requirements when valuable*.—Based on the functions of a business, its vertical industry and public or private ownership, there are a variety of reporting requirements that businesses have to shareholders, customers, partners, the government and others. As reflected in the enabling legislation, efforts should be made to acknowledge and existing reporting activity where appropriate so as to avoid duplication and excess effort. Certification activity may be able to "piggyback" on some existing auditing efforts.
- *The program should support self-assessment by businesses as well as external second party and third party assessments*.—Businesses should be able to apply elements of the program to self-assess their operations and self-declare (first party assessment) as well as utilize it in assessing related parties such as suppliers (second party assessment). Third party certification by unrelated certifiers should also be an option. First, second party and third party assessments could be valuable in assuring business preparedness in supply chains.
- *The corporate governance & corporate social responsibility (CSR) areas should be evaluated for past lessons learned and possible synergies with the voluntary certification program*.—In an increasingly risky business environment, risk management is a growing concern among boards of directors and executive management. The voluntary certification program might potentially be structured to address these concerns at least in part by assessing the state of business preparedness.
- *In designating one or more preparedness standards for use in the program, a constellation of standards or framework approach should be evaluated. An umbrella standard should be considered in this regard to assure core consistency among various standards*.—There are multiple preparedness guidance documents with significant value to one or more business sectors. Some are general or program level; others may be more functionally oriented, for example, risk assessment-focused. Consideration should be given to structuring a certification process which accommodates the assessment of the business against one or

more standards but in a unified framework. Such a framework could acknowledge a common core of program elements potentially utilizing an "umbrella standard."

- *The program and chosen standards should be applicable on an international basis to have the most value to multinational corporations*.—The program may involve a number of standards, but whichever standards are chosen, they should be capable of being applied on an international basis in order to accommodate the needs of multinational firms.
- *Special considerations should be made for small businesses that wish to pursue voluntary certification. The involvement of industry associations and large-to-small business mentoring should be considered*.—Clearly not all small businesses will see value in pursuing the voluntary certification. This is to be expected. For those that do, the new certification program must be economically and operationally achievable. Separate classifications and methods of certification for small businesses should be established as appropriate and in consultation with small business representatives and organizations. Supply chain mentoring should be explored to consider how larger companies might assist their critical suppliers that are small businesses.
- *Potential "incentives stakeholders" should be welcomed into the process from the beginning to assure that the voluntary certification program has value to them in potentially acknowledging and rewarding business preparedness efforts*.—A major rationale cited in the testimony for the program was the need to enable a closer link between preparedness and benefits for business. Key stakeholders in such areas as supply chain management, legal liability, insurance and rating agencies have generally concurred that business preparedness is valuable and should be acknowledged more widely but to date there has been no generally accepted methodology to confirm that preparedness exists in a business so that it could be acknowledged. This program could supply such a method, and so the process should involve these potential incentives stakeholders as well as others early in the development of the program. Following are considerations in this regard:
  - *As rating agencies potentially widen their review of enterprise risk management in their analysis of businesses, the rating agency perspective should be invited into the development and ongoing operation of the certification program*.—This could potentially facilitate greater recognition of effective corporate preparedness. Rating agencies are increasingly focusing on enterprise risk management in their analysis including business continuity and emergency management programs by the corporation. Including rating agency input into the voluntary certification program might allow for these agencies to acknowledge this voluntary certification more readily in their own analysis and thereby effectively reward preparedness by corporations.
  - *Supply chain resilience is a growing concern among corporations. The voluntary certification program offers value in assessing supplier resilience. The supply chain management perspective should be included in the development and ongoing operations of the certification program.*—There is an increasing focus on supply chain resilience and the preparedness of critical suppliers. Firms frequently require supply partners to adhere to certain preparedness requirements. Some firms promote preparedness-related best practices through mentorship, training, education and joint exercises with supply partners. Corporations are looking for tools to assess the resilience/reliability of the suppliers of critical goods and services. From the supplier perspective, some firms are noting significant time spent on interfacing with multiple customers assuring each of the business' preparedness status. A voluntary certification program could potentially provide a commonly-accepted verification of preparedness and thereby avoid multiple customer queries. Similarly, customers could use the certification to minimize their supply assessment efforts.
  - *Insurance company and related input should be incorporated into the voluntary certification program to support increased recognition of business preparedness in the future*.—It can be argued that the insurance industry on the whole understands the general value of business preparedness to minimize losses to both the individual businesses and the insurance company. However, how and if insurance companies measure preparedness varies significantly. Current efforts to correlate preparedness actions to loss reductions are largely focused on property risk. The insurance market is stratified, with larger companies receiving relatively more attention and greater flexibility from underwriters than smaller companies. A commonly-accepted third party assessment of business preparedness could be a valuable indicator of risk which might be used by insurance companies in their underwriting potentially. This could

possibly result in a greater recognition of preparedness in the future. The audit processes involved with the certification program may provide underwriters with data they cannot access otherwise due to lack of time or expertise, helping them to systematize their understanding of business continuity. In addition, a voluntary certification program could also begin to build a historical record that over time could inform a closer understanding of what preparedness measures best minimize future insurance claims. Challenges that need to be addressed include how preparedness standards would fit into underwriting guidelines. State insurance regulators may also consider how to promote the incorporation of elements of the certification program in the underwriting process. Another possibility for driving the development of insurance incentives for preparedness is to approach it from a consumer demand standpoint. Insured companies may take individual and/or collective action to demand acknowledgement of preparedness efforts by insurers.

- *Representatives from the corporate counsel and wider legal community should be incorporated in the development and implementation process of the program to support a potential role of certification in minimizing legal liability for the impacts of emergencies*.—Negligence tort and other legal liability can be a major exposure for companies of all sizes in the aftermath of an emergency. When another party is impacted by the event, it is often argued that the company did not do enough to prepare for emergencies. Yet, it can be difficult to ascertain how much preparedness is enough given the diversity of risks that face a company. Advance and documented compliance with an established recognized standard for preparedness can serve to support an affirmative defense to liability claims after an emergency. The certification program will be centered on voluntary compliance with one or more industry standards. Thus, the certification program should optimally be structured to minimize legal liability of the business which pursues preparedness in compliance with it. The development of statutory guidelines would provide additional legal motivation to pursue certification. On the other hand, there is a potential disincentive pertaining to undertaking preparedness certification and the related documentation of preparedness actions undertaken by a company, especially with respect to the identification of risks to the company and its current vulnerabilities. Legislation providing safe harbor from litigation to any certified firm would provide a major incentive for certification, as would the development of what is called "self-evaluative privilege" to ensure that the findings of the certification process would not be used in court against a proactive corporation.

Ms. JACKSON LEE. Thank you very much for your testimony.

I now recognize Dr. Stephens for 5 minutes. Dr. Stephens, you may also summarize your statement and be recognized for 5 minutes. Thank you.

STATEMENT OF DR. KEVIN U. STEPHENS, M.D., DIRECTOR, HEALTH DEPARTMENT, CITY OF NEW ORLEANS

Dr. STEPHENS. Thank you, Chairwoman Jackson Lee, the Ranking Member Lungren, and other members of the committee and guests.

Thank you for your invitation and, of course, your most gracious introduction.

New Orleans is one of America's most beloved and culturally distinctive cities. As you are all aware, it has faced many challenges in recovery and the rebuilding after the—and perhaps our worst natural and manmade disaster to occur in the United States of America.

Please know that I speak for our entire community when I say that we are grateful for all that Congress has done. We are very happy to have you help us recover from Hurricane Katrina and the subsequent flooding. We are truly appreciative of your continued concerns about our progress in caring for our citizens, while we

work diligently towards resolving our longer-term recovery challenges.

Thank you for providing this opportunity for us to share with the committee our unique perspective on the concept and implementation of resilience, particularly regarding the critical health care infrastructure of a community.

Being resilient means having the ability to withstand a blow and to bounce back, a capacity which must be built on an already-solid foundation. Our community suffered a catastrophic disaster that destroyed most of its private and public health care infrastructure when the levees broke, flooding 80 percent of the land area in our city.

We continue to struggle to rebuild the health care foundation and cover basic medical needs for our citizens. We still have excessive waits at our emergency rooms. We have a shortage of mental health inpatient beds. We have a lack of primary care clinics to provide day-to-day health care for the indigent and uninsured and minimal medical surge capacity, even though we are ranked high in vulnerability, in terms of terrorism and natural disaster.

Below are some of the major challenges we have encountered to building resilience in the greater New Orleans health care community, as well as some suggested solutions.

One of our challenges in the recovery and building resilience that plagues our health care providers is the duality that they face, as victims, as well as responders in a critically needed system. It is quite difficult to play both of these roles simultaneously.

Many of our providers lost everything, including their offices, their medical diagnostic equipment, medical and financial records, and their homes. Provisions must be made for providers to resolve their personal difficulties before they can begin to provide critically needed services.

Even for those providers and institutions left standing after the disaster, a significant number of them experienced losses in revenues and a scattering of their patients. Many of our regional hospitals decided not to re-open their facilities, and those that remain have a drastically reduced number of inpatient beds.

This reduced capacity and capability has left doctors with no place to admit their patients. Faced with a decreased population pool and no reliable source of income, many had no choice but to relocate, resulting in a further damage of an already decimated health care system.

It should be noted that several local and regional hospitals stayed open and re-opened immediately following Hurricane Katrina. These hospitals have incurred tremendous financial losses, primarily due to the number of increased patients of uninsured individuals seeking health care.

While we owe a debt of gratitude to our community partners for assisting our citizens in a time of need, financial relief needs to occur for these institutions to continue to provide quality health care services.

Many of our private-sector hospitals realized that rather quickly following Hurricane Katrina that their financial risks were tremendous. These institutions faced higher labor costs, higher insurance

costs, higher provider cost, higher uninsured numbers, and higher construction costs.

It was evident that if they re-opened that they would be likely to lose millions of dollars. Hence, four of our regional health care facilities have decided not to re-open.

As mentioned earlier, in providing care in the increasing indigent and uninsured population, due to dislocation, job loss, and other financial woes stemming from the disaster, has been one of the greatest financial liabilities in our private hospital facilities.

Federal laws require emergency departments to accept and treat patients regardless of their financial capability. With the collapse of a State-run charity system immediately after the hurricane, private hospitals were forced to assume the care of the uninsured.

Some compensation for these services was provided by the State at a later date, however, but according to many CEOs it has been late in coming and woefully inadequate.

Following Hurricane Katrina, there was no readily accessible database of patient health information available to providers. But we would like to thank the American Medical Association and other organizations who put together a database that enabled patients to access their pharmacy information and get badly needed prescriptions filled.

While this database proved to be an invaluable service, much more health information is needed in a disaster situation in order to provide excellent care to our citizens.

So we have just basically three solutions, starting with the patients. It would be great to develop a national continuity of care record system, which would allow patients to access critical health care information at the time of a disaster.

Entrepreneurs have also identified this and are flooding the market with various forms of mobile personal data archiving systems. While many health care provider associations have agreed to the critical fields in a continuity of care record, a federally standardized approach is warranted.

One must ask: Why we can access our e-mail accounts, banking information, and other critical data while we are abroad, but no such means for accessing our medical data exists?

No. 2, for our providers, some of our action reviews that were performed after Hurricane Katrina response cited a need for a mechanism where providers can easily access across State boundaries in a response to a disaster.

An avenue for expediting medical licenses and certifications needs to be in place to facilitate the credentialing and responding health care providers. A national practitioner database could be used to meet this goal.

While we are aware of the Department of Health and Human Services, that they created the Emergency System for Advance Registration of Volunteer Health Professionals in response to 9/11, we need more emphasis linking various States, because this is primarily a State-run program. We need a national registry of providers.

For the hospitals, the health care community is pleading for a more reliable and predictable reimbursement mechanism for pro-

viders and hospitals that respond to a disaster, as declared by the president.

The private sector must also have some assurances upfront that they will be reimbursed for their contributions. Health care services can be quite costly, and the health care community should not be expected to absorb all of the expenses incurred after a disaster.

For example, Medicaid payments should be made portable during the time of a declared disaster so that health providers in another State——

Ms. JACKSON LEE. Mr. Stephens, if you could—I don't know how much more you have. If you could summarize for us, please. Thank you.

Dr. STEPHENS. Yes. The other stats would basically give full faith and credit to their whole State Medicaid insurance card.

Finally, we do acknowledge that we have a whole lot of initiatives organized and authorized by Congress in the UASI and the metropolitan response system. They are underfunded, and we will suggest that they will be continued funding for the local and State agencies.

So thank you very much for allowing me time to speak, and I look forward to your questions.

[The statement of Dr. Stephens follows:]

PREPARED STATEMENT OF DR. KEVIN U. STEPHENS

MAY 14, 2008

Chairman Thompson, Ranking Member King, Chairwoman Jackson Lee, Ranking Member Lungren, and other distinguished members of the committee and panel: I am Dr. Kevin U. Stephens, Director of the New Orleans Health Department. New Orleans is one of America's most beloved and culturally distinctive cities, but as you are all aware, it is facing the challenge of recovering and rebuilding after the worst natural and man-made disaster to occur in the United States of America.

Please know that I speak for our entire community when I say that we are grateful for all that you in Congress and that the people of the United States have done to help us recover from Hurricane Katrina and the subsequent flooding. We truly appreciate your continued concern about our progress in caring for our citizens while we work diligently toward resolving our longer-term recovery challenges.

Thank you for providing an opportunity for us to share with the committee our unique perspective on the concept and implementation of resilience—particularly regarding the critical healthcare infrastructure of a community. Being resilient means having the ability to withstand a blow and to bounce back—a capacity that must be built on an already solid foundation. Our community suffered a catastrophic disaster that destroyed much of its private and public healthcare infrastructure when the levees broke, flooding 80 percent of the land area of our city. We continue to struggle to rebuild the healthcare foundation and cover the basic medical needs of our citizens. We still have excessive waits at our emergency rooms, a shortage of mental health inpatient beds, a lack of primary care clinics to provide day-to-day healthcare for the indigent and uninsured, and minimal medical surge capacity, even though we are ranked high in vulnerability for terrorism and natural disasters.

Below are some of the major challenges we have encountered to building resilience in the Greater New Orleans Healthcare community, as well as suggested solutions.

CHALLENGES

One of the challenges to recovery and building resilience that plagues our healthcare providers is the duality they face as victims as well as responders in a critically needed system. It is quite difficult to play both of these roles simultaneously. Many of our providers lost everything, including their offices, medical diagnostic equipment, medical and financial records, and their homes. Provisions must be made for providers to resolve their personal difficulties before they can begin to provide critically needed services.

Even for those providers and institutions left standing after the disaster, a significant number experienced loss of revenues and a scattering of their patients. Many of our regional hospitals decided not to reopen their facilities and those that remain have a drastically reduced number of inpatient beds. This reduced capability has left the doctors with no place to admit their patients. Faced with a decreased population pool and no reliable source of income, many had no choice but to relocate, resulting in further damage to an already decimated healthcare system.

It should be noted that several local and regional hospitals either stayed open or reopened immediately following Hurricane Katrina. These hospitals have incurred tremendous financial losses primarily due to the increased number of uninsured individuals seeking healthcare. While we owe a debt of gratitude to our community partners for assisting our citizens in a time of need, financial relief needs to occur in order for these institutions to continue to provide quality healthcare service.

Many of our private sector hospitals realized rather quickly following Hurricane Katrina that their financial risks were tremendous. These institutions faced higher labor costs, higher insurance costs, loss of providers, higher uninsured numbers and higher construction costs. It was evident that if they reopened, they were very likely to lose millions of dollars. Hence, four of our regional healthcare facilities have decided not to reopen.

As mentioned earlier, providing care to the increasing indigent and uninsured population (due to dislocation, job loss and other financial woes stemming from the disaster) has been one of the greatest financial liabilities to our private hospital facilities. Federal laws require Emergency Departments to accept and treat patients regardless of their financial capability. With the collapse of the State-run "Charity" system immediately after the hurricane, private hospitals were forced to assume the care of the uninsured. Some compensation for these services was provided by the State at a later date, but according to many CEOs it has been late in coming and woefully inadequate.

Following Hurricane Katrina, there was no readily accessible database of patient health information available to providers. We would like to thank the American Medical Association (AMA) and other organizations that put together a database that enabled patients to access their pharmacy information and get badly needed prescriptions filled. While this database proved to be an invaluable service, much more health information is needed in a disaster situation in order to provide excellent care to evacuated citizens.

SOLUTIONS

Some of the after-action reviews that were performed on the Hurricane Katrina response cited the need for a mechanism where providers can easily cross State boundaries in response to a disaster. An avenue for expediting medical licenses and certifications needs to be in place to facilitate the credentialing of responding healthcare providers. A national practitioner database could be used to meet this goal. While we are aware that the Department of Health and Human Service's (HHS) created the Emergency System for Advance Registration of Volunteer Health Professionals (ESAR–VIP) program in response to September 11, more emphasis needs to be placed on the agency's ultimate goal of linking these various State-managed ESAR–VIP programs into one national database. This will ensure that healthcare providers are not caught in bureaucratic red tape when citizens are in need of the services that they can provide.

The healthcare community is pleading for a more reliable and predictable reimbursement mechanism for providers and hospitals that respond to disasters declared by the President. The private sector must have some assurances up front that they will be reimbursed for their contributions. Healthcare services can be quite costly and the healthcare community should not be expected to absorb all of the expenses incurred. For example, Medicaid payments should be made portable during the time of a declared disaster so that health providers in another State could receive reimbursement for services rendered. One possible way to achieve this would be for States to give full faith and credit to the Medicaid insurance card from the disaster affected locality. The host State would allow their providers to bill their Medicaid program for the care of evacuees. The host State Medicaid program would then bill the disaster-affected State for reimbursement. This would also allow for evacuees to obtain medical care as well as medications in the event of an evacuation.

The Nation should develop a national CCR (Continuity of Care Record) system which would allow patients access to critical health information in the time of a disaster. Entrepreneurs have also identified this need and are flooding the market with various forms of mobile personal data archiving systems. While many healthcare provider associations have agreed to the critical fields needed in such a record, a

federally standardized approach is warranted. One must ask the question why we can access our email accounts, banking information and other critical data while we are abroad, but no such means for accessing our medical data exists.

It is important for Congress to authorize and continue to fund the major grant programs that communities use to build resilience into their critical infrastructure. Programs such as the Urban Area Security Initiative (UASI), and the Metropolitan Medical Response System (MMRS) support medical surge capacity, mass fatality prophylaxis, and other key needs. Specific to the healthcare community, the Hospital Preparedness Program (HHP), under the U.S. Department of Health and Human Services, is a key provider of funding for hospitals and healthcare systems' all-hazards preparedness and response capability. During the past five funding years of the HPP grant, significant improvements have been made in our area regarding interoperable communication, surge capacity, decontamination capabilities, training, and education. It is important to note that funding for these programs has been reduced and their existence is constantly threatened every budget year. For our community, the current allocation of funds for healthcare preparedness as well as additional financial support is needed to bring our healthcare infrastructure back.

We also advocate that Congress make provision for communities hit by catastrophic disasters to have automatic access to funding to rebuild what is lost or damaged by a disaster. Our Office of Emergency Preparedness is faced with the daunting task of redeveloping our medical surge, decontamination, triage and prehospital treatment capabilities utilizing the MMRS grant. Many of the non-disposable items that were purchased by this grant to support the 11 Target Capability Focus Areas, outlined in the MMRS grant guidance document, were either utilized or destroyed during the aftermath of Hurricane Katrina. Additional grant dollars would greatly assist this initiative to return our city's level of preparedness to our pre-Katrina standards.

CONCLUSION

Ladies and gentlemen, thank you for allowing me to speak with you on the status of our recovery and the challenges we and the Nation face to make our homeland more resilient. I believe the proposals outlined in this document will accelerate our recovery and assist others to rebound faster and more effectively after a disaster of catastrophic proportions. We thank you, the Homeland Security Committee, the Subcommittee on Transportation Security and Infrastructure Protection and Congress, for your continued support as we rebuild our city and region. Though we still face historic challenges, we are hopeful that with your assistance, we can solve the remaining problems and build a better and stronger community for everyone.

Ms. JACKSON LEE. I thank you very much for your testimony. I thank all the witnesses for their testimony.

I remind each member that he or she will have 5 minutes to question the panel.

I now recognize myself for 5 minutes.

Assistant Secretary Stephan, we hear the number 85 percent over and over again of the critical infrastructure that is owned and operated by the private sector. Among that 85 percent, with what percentage of the Department continuously engage for critical infrastructure security purposes?

Because many of these assets are not regulated for security purposes, what is the business case the Department makes to these entities to secure their assets? What are the carrots you use to get them to do the right things?

Do you encourage the private sector to be resilient and be able to bounce back to effective operations? How do you do that?

Colonel STEPHAN. Yes, ma'am. To answer your first question, I do not have an exact percentage for you, but we routinely engage with all 17—actually, now 18 critical infrastructure sectors that are defined in the National Infrastructure Protection Plan from communications, electricity, oil and gas, I.T., transportation, you name it.

We have sustained governance mechanism that allows very frequent meetings between our different entities, as well as an information sharing, where virtually every day we are passing either threat information or operationally-related information, based upon what is happening with our infrastructures on a daily basis, train derailments, bridges collapsing, the wildfires in California and Florida that we are monitoring today, ongoing activities and relationships.

Resiliency is built in as part of our organizing framework, in terms of national level documents that we have built in voluntary partnership with the private sector over the past 3 years, all the way down to our facility-level security plans and buffer zone security plans that resiliency, redundancy, robustness, redundant command post-type considerations that are built into those frameworks.

The other piece on incentivization, as Congressman Lungren pointed out, the threat piece is key. We can bring a lot of people to the table with respect to providing them information on what exactly the threat is.

If we have an emerging, credible threat in the sector, we do everything we can to develop tearline information with the intelligence community, get it into the hands of the owners and operators.

Where we don't have that type of information, we have got a special team of analysts in my shop, and Charlie Allen's shop, that work on lessons learned from abroad. If the terrorists start attacking hotels and discos and transit systems here, they are certainly doing it abroad almost every day somewhere. Iraq, Afghanistan, Indonesia, Jordan, Egypt, you name it, there they are.

We are capturing those lessons learned, learning the techniques and procedures, and exporting that information across our private-sector information network.

Ms. JACKSON LEE. Let me quickly ask another question. You have submitted a lot of documents. Do you have an internal white paper or managerial directive dealing with infrastructure protection that define resiliency and how it is going to be implemented?

If you have those, we would like to have those submitted to the committee.

Colonel STEPHAN. Yes, ma'am. The definitions of protection and resiliency and all of its other components are included in the National Infrastructure Protection Plan that I have provided or brought with me today to submit to the committee.

Ms. JACKSON LEE. Do you have how it can be implemented? Is that——

Colonel STEPHAN. Ma'am, it is all part and parcel of the framework. For me, this is all about trying to drive—not you, not members of this committee, but there are academics and think-tanks out there that would like to drive a wedge and cause us to make a choice between protection, prevention, and the response and recovery side, or the resiliency side.

I would argue, as I heard you also argue, ma'am, in your opening testimony, there isn't a choice to make. It is how do we combine the two imperatives, how do we blend them? On the prevention and protection side, we have to do it on a risk-based approach or else

we could be spending a lot of resources, a lot of money in areas that don't provide bang for the buck.

We are not for that. Risk-based approach to the upfront components, combined with the capability to absorb a strike and respond adequately, that is what this Nation is all about.

Ms. JACKSON LEE. Well, let me get Mr. Czerwinski and Mr. Johnson, Mr. Raisch, to respond to that.

Mr. Czerwinski.

Mr. CZERWINSKI. Thank you, Madam Chairwoman. The Assistant Secretary makes a very clear and important point, that is, that the balance is critical.

The way in which resilience ought to be considered in this context of the private sector is that risk has changed to the point where prevention, yes, is critical and protection is indispensable, but the resilience component has to evolve to reflect the interconnectivity between the different sectors themselves, so that, as we go through the process of educating the sectors about the threats that they face and the risks that are peculiar to those different sectors, the other side of the coin is for us to identify the ways in which these different sectors are actually interdependent themselves.

I know there are already efforts underway in this domain. But there could be a great deal that we could gain from a framework that might develop the information-sharing to the next level, such that there is different kind of resiliencies evolved.

The redundancy is a part of it that the Federal Government has to embrace, but the redundancy is not the sort of thing the private sector is going to be too enthusiastic about. So there is still some opportunity to drill into that.

Ms. JACKSON LEE. You think that the Federal Government can do a better job?

Mr. CZERWINSKI. Well, I am an American citizen. I always think the American government can do a better job. But I think the—I think the Department of Homeland Security has been given the authority and freedom to work with the private sector and has created some engagement mechanisms that enable that. We participate in some of them at IBM.

The way in which the opportunity resides, though, I think, is actually to look at this framework that embraces a broader picture of human capital technology and governance, not just threat information.

Ms. JACKSON LEE. If we can't get the private sector to give us a good give-and-take, Mr. Czerwinski, we can't get to a better product.

So, Mr. Johnson, please don't hold back. We are not here to sugarcoat, nor are we here to suggest that Colonel Stephan does not have a strong constitution and can accept constructive criticism. So we would like to see what your thoughts are, please.

Mr. Johnson.

Mr. JOHNSON. Thank you, Madam Chair.

The issue of resiliency in the financial services sector is one that is longstanding. In fact, we are, in some ways, a bit of a unique sector in that, in order to efficiently operate, every one of the competitors in our private sector must trust each other to operate effi-

ciently as we pass money around the system. Indeed, it goes out beyond the United States.

So resiliency is really core to what we do, and we are only as strong as our weakest link. So we have to always ensure that we are resilient in what it is we do, because we are so interconnected.

That is different, potentially, in other sectors. As far as what the public sector can do or do better, I don't have a strong point of view that that is anything that needs to be done in addition. I think most of what I see is the private-sector organizations realizing how important resiliency is in what it is we do every day and spending money because it is the right thing to do.

Ms. JACKSON LEE. Is that the industry spending money?

Mr. JOHNSON. That is the industry spending money.

Ms. JACKSON LEE. Can the government do more in assisting that? Is there the interaction between the government on resiliency with the private sector from the financial services' perspective?

Mr. JOHNSON. On financial services, there is a great relationship between us and our sector-specific agency, which is the U.S. Treasury. Lots of discussions about, as Secretary Stephan said, a prioritization on the front end, or risk assessment on the front end for protection, as well as a resiliency perspective on day-to-day operations.

Ms. JACKSON LEE. Well, can you point us to written documents where you have received from the U.S. Department of Treasury that focuses on resiliency? Do you have those?

Mr. JOHNSON. I do not have those with me, no, but I can provide you guidance that comes from the Federal Government, as well as our sector-specific plan—thank you, Secretary Stephan—which articulates across the entire sector, from banking to insurance.

Ms. JACKSON LEE. Well, let me do this. I mean, a document that has already been submitted into the record is fine. The question is whether there is interaction that focuses on resilience.

Let me yield to Mr. Raisch. I thank you for your answer, so I can yield to the distinguished ranking member from California.

Mr. RAISCH. Thank you, Chairwoman.

A few very brief comments. I would say, firstly, I don't think it is an either-or, prevention versus resiliency. This is a continuum. I mean——

Ms. JACKSON LEE. We agree on that.

Mr. RAISCH. Got that.

Ms. JACKSON LEE. But we want to know whether the Federal Government can do better. That is what we would like to hear.

Mr. RAISCH. Certainly, and I would think the Assistant Secretary would agree, we can always improve.

Ms. JACKSON LEE. The secretary is not the singular representation of the Federal Government. So I know you are sensitive to his presence on the panel.

Mr. RAISCH. Very good. I think we can all do more to leverage the economic rationale. We can call for business and government to do—to be more prepared. Quite frankly, that is right up there with apple pie, mom and pop, and so forth.

At a certain point, businesses have a responsibility to their stakeholders to essentially make rational economic choices. As such, I think DHS and other elements of government, Congress in-

cluded, can help clarify some of the business case incentives, develop, perhaps, new ones.

As I mentioned in my testimony before, I think this certification program that was recently passed has an opportunity to link good practice with direct economic benefits in a way that has not happened in the past. We have directly worked in the past with elements of, if you will, the external stakeholders, those being insurance, rating agency, legal liability community.

Many of them are disposed towards acknowledging resiliency, but have not had an effective measure to date to acknowledge it. If you can't acknowledge it or measure it, you can't reward it.

So I think there is a real opportunity in moving forward this voluntary certification program, particularly with an emphasis towards economic value to business.

Ms. JACKSON LEE. I thank you.

Dr. Stephens, I am going to hold my questions for you.

I yield to the distinguished gentleman for his time of questioning from California.

Mr. LUNGREN. Thank you very much.

I think the panel is to be commended for resisting the temptation to treat Colonel Stephan as a piñata here.

Colonel, I happen to think that you have done a very good job and the Department has done a good job in launching this effort. That is what we have done: We have launched the effort. There still remains a lot to be done.

Mr. Johnson, you made a very obvious point, but something that we often overlook. The very nature of the financial services industry is one of dependence on resilience. I mean, if you go down for a day or two, your business essentially has been drastically punished or suffered. I would say the same thing with the communications industry, for instance.

But when we get into some of the other industries, I don't think the resilience aspect is as obvious and, therefore, as obvious to the bottom line and, therefore, as justifiable to shareholders. It seems to me that is the nexus that we need to sort of reach.

So let me posit this question to you, Mr. Raisch. Is that the proper way to pronounce Mr. Raisch?

Mr. RAISCH. Yes.

Mr. LUNGREN. Mr. Czerwinski.

Let's presume the government—the answer is not going to be a lot more government money. Let's just set that aside, because that is an easy one to say. "Well, we will give you more grants. We will do this."

Setting aside money, what are the kinds of things that can most effectively, efficiently and quickly allow that kind of economic value to be realized by sectors other than the financial services sector or the communications sector?

I mean, what are the keys to getting other parts of American industry to have resilience as a part of—and it is more than resilience, it is also protection and prevention from terrorist attack or natural disaster?

Mr. CZERWINSKI. Well, I will go first. Thank you for that question. This gets to the real critical point, which is, how does this issue become portable across different sectors?

What we tried to look at, actually, was the cargo container, flow of cargo and container traffic across maritime, for example, if you were to take that, you could look at this from a double bottom-line concept, where there is a way in which you could find economic efficiencies to create better system visibility, that is, understand what is going on from end to end for a container cargo ship.

That is obviously useful from a regular bottom-line perspective, because it gives you the understanding of where disruptions exist or inefficiencies are.

But if you look at this from a double bottom-line, that is, the resiliency component, that same system visibility—which, by the way, is never perfect, and usually that information resides in different sectors—could also enable this decisionmaker to say, "This disruption is actually unique. This is not a situation where we are looking at a derailment of a certain cargo, but we are looking at something completely new."

Without the ability to have that visibility, that decisionmaker wouldn't be able to say, "We need to react differently," or, "We need to re-route this," just taking the cargo one, for example. So in that case, you could have both resiliency and efficiency resulting in a double bottom-line.

I hope that answers your question.

Mr. LUNGREN. Mr. Raisch.

Mr. RAISCH. In reference to really the governmental role that can add a new equation to this, I think—let's look at businesses. They are organized as individual organizations and, as such, that is their focus primarily.

I think government can bring a wider perspective. I think we have touched on some other issues where we looked at critical dependencies across sectors and across businesses and so forth.

The reality of this is, right now, globalization is most compelling bottom-line argument for a lot of resilience. Organizations that we deal with daily have supply chains that reach from here through Mumbai in India to Shanghai and back again.

As such, I think businesses are learning the lesson, to the extent they have a wider geographic footprint, if you will, for any one adversity, whether the manmade or natural disasters to occur.

But I think government can play a role in perhaps distilling some of those lessons, reinforcing also the ability to cross-pollinate across various elements of business. There is a lot of good learning that has happened, particularly in the critical infrastructure areas, under Assistant Secretary Stephan, but also, quite frankly, I think cross-pollination across those sectors, those 18 sectors now, can be facilitated.

I think the ability to, again, communicate in some common elements of preparedness, defining, if you will, as I mentioned earlier, that Rosetta Stone. I think this—again, getting back to this certification program, I think that offers a tremendous opportunity to do so.

So I think facilitating crosspollination across various sectors, so we are sharing our insights in an effective manner, providing an understanding of the societal dependencies, that certainly the experience in New Orleans underscored dramatically, that no company,

no entity, no household is an island, and, in fact, we are all very much integrated.

I think that is very much a governmental role in that respect and one that, I think, provide assistance. The other thing, I think, on a low-cost basis, I think the provision of some common tools, based upon those key elements, preparedness.

In this electronic environment—and there are some good things being done now on ready.gov, but I think we can move forward and have a truly robust resource from an electronic or Web-based environment that facilitates business preparedness across the Nation.

Mr. LUNGREN. Dr. Stephens, I asked the others not to consider money, but I want to change that with respect to a question for you, and that is that, on the Federal side, we have, in terms of the reimbursement we give to hospitals and medical institutions, factored in a number of different things. We have factored in and factored out costs of education, training, et cetera.

Is there, on the part of the Federal Government, in terms of reimbursement for expenses by medical institutions, particularly hospitals, any consideration at the present time of the resiliency factor, and particularly, if we do an analysis of a hospital, and we try and analyze whether or not there are sufficient beds to take care of a pandemic or other natural disaster?

Dr. STEPHENS. No, unfortunately, we don't take that into consideration, in terms of resiliency. In New Orleans particularly, we are so busy trying to just mine day-to-day that to get to resilient is not high on the radar.

I think it should be, though, because I think that the ability to respond in the midst of a disaster is dependent upon your ability to have resilience.

Mr. LUNGREN. See, I recall over about a 25- or 30-year period of time Federal Government decisionmaking drove hospitals to be more "efficient" and, in the process, we actually caused hospitals to reduce the number of available beds they had.

One of the ways we did that was making sure the patients got up sooner, rather than later. I have seen it in communities across America.

We prided ourselves on making our health care system more efficient, and one of the indices was, hey, we have fewer beds sitting out there. That is great, unless you need the beds.

So I think one of the things we have to deal with from a governmental standpoint is, as we have tried to make the medical system more efficient, we have created conditions that, if we have a tremendous impact on a health care system in a particular area, we don't have the infrastructure we had 40 years ago when we had so many beds available. I am not sure we have totally dealt with that question.

Dr. STEPHENS. Your point is highlighted with the mental health beds. You not only in New Orleans, in the State of Louisiana, we have basically zero availability of mental health beds, so our patients have to be transferred out-of-State to get resources. That is private and public, so that point is well taken.

Mr. LUNGREN. I yield back the balance of my time. Thank you.

Ms. JACKSON LEE. I thank the gentleman and yield myself an additional 5 minutes.

Dr. Stephens, can you tell me how many hospitals, public and private, were in New Orleans prior to Hurricane Katrina?

Dr. STEPHENS. Approximately 11.

Ms. JACKSON LEE. What do you have now?

Dr. STEPHENS. Open, we have four.

Ms. JACKSON LEE. Okay. Do you have a public Charity Hospital open?

Dr. STEPHENS. Yes, we do. We have University Hospital, which is our Charity Hospital.

Ms. JACKSON LEE. The hospital—one of the hospitals that was open before that is now closed, was that a Charity Hospital? You indicate you had 11; there are now four.

Dr. STEPHENS. Yes. One of the hospitals—Charity Hospital has had two hospitals, University, and the old Charity, as we knew it.

Ms. JACKSON LEE. It was open prior to——

Dr. STEPHENS. Yes, they both were open.

Ms. JACKSON LEE [continuing]. Katrina?

Dr. STEPHENS. Now, only the University Hospital, which has, as I understand it, maybe 200 beds is open now.

Ms. JACKSON LEE. I didn't hear you. Pardon me?

Dr. STEPHENS. University, University Hospital.

Ms. JACKSON LEE. Has how many beds?

Dr. STEPHENS. Two hundred.

Ms. JACKSON LEE. How many did Charity have?

Dr. STEPHENS. Totally, they had 539, as I recall.

Ms. JACKSON LEE. Is that building still standing?

Dr. STEPHENS. It is still standing.

Ms. JACKSON LEE. All right. So, in actuality, if we looked at the practicalness of what has happened, you had 11 hospitals pre-Hurricane Katrina, is that correct?

Dr. STEPHENS. That is correct.

Ms. JACKSON LEE. You now have four?

Dr. STEPHENS. Correct.

Ms. JACKSON LEE. Now, one could put on the record that you obviously have had a decrease in population, but I assume that every effort that the city government is making and corporate fathers and mothers are to build back your population by many returning New Orleanians?

Dr. STEPHENS. Correct.

Ms. JACKSON LEE [continuing]. People from New Orleans, is that correct?

Dr. STEPHENS. That is correct.

Ms. JACKSON LEE. So, in essence, if you were to go back to full capacity of your population, you would have and may have now a health crisis?

Dr. STEPHENS. We do. We currently have a—in fact, to go from beds, we had 2,250 beds available in New Orleans before Katrina. Now we have less than 1,000 available.

Ms. JACKSON LEE. There was a MASH unit that was in, I believe, the Hyatt. Has that been closed?

Dr. STEPHENS. Yes, it has been.

Ms. JACKSON LEE. Where do those patients now go?

Dr. STEPHENS. To the University Hospital system, which is the 200-bed facility that I mentioned.

Ms. JACKSON LEE. Would you suggest that your health system is at capacity or even beyond?

Dr. STEPHENS. Yes, we are bursting at the seams. We have basically no available beds anywhere in the city.

Ms. JACKSON LEE. So what could have been—and you have made your appropriate statements. We thank you for recognizing the hard work of this Congress in a bipartisan way. We accept that.

But what could have been more effective from a resilience perspective, one, as you look at it, as a medical professional, what could have been done pre-Katrina, but now, as we look at post-Katrina, resilience also is the ability to get back in operation?

Where did the resilience aspect of fixing the health care system in New Orleans fall after Hurricane Katrina? What was missing to put you in near-capacity?

Dr. STEPHENS. Well, I think the big thing is reimbursement, the predictability and reliability of reimbursement.

We had several hospitals that opened up, but we couldn't tell them, for the uninsured, when our Charity Hospital system closed, we had a lot of uninsured patients that would show up at your doorstep.

There was no predictable, reliable way that hospitals would know, "If I treated this person, I would get $1 or anything for treatment of this patient," because—laws require that, if somebody shows up in your emergency room, you have to see them, but there are no revenues associated with that treatment.

So without having a predictable, reliable source of income, the private-sector hospitals chose not to open, because the hospitals that stayed open—I think I heard like $135 million was lost last year among five hospitals that were open.

So without a predictable, reliable source of income, the private sector says they are for-profit, they have to show——

Ms. JACKSON LEE. But there is an aspect to resiliency that deals with a revenue stream.

Dr. STEPHENS. Absolutely.

Ms. JACKSON LEE. So, if we were to look at that sector, we need to be assured that we have an immediate revenue stream or some bridge that would keep them going?

Dr. STEPHENS. Absolutely.

Ms. JACKSON LEE. What was the difficulty in opening—what was the missing resiliency that would allow you to have opened the other Charity Hospital with 539 beds?

Dr. STEPHENS. Well, the other Charity Hospital, as I understand it, from the flooding, we had structural integrity problems. In fact, there is a group now—looking at that facility to see what impediments are preventing this one from being opened or not.

But it was an old facility, grant you. They had many problems. But I am not really sure. That is a very hot potato, if you will.

Ms. JACKSON LEE. But there was no capacity for you to sign or to collaborate to have other resources to immediately find a substitute location for those 539 beds?

Dr. STEPHENS. That is correct.

Ms. JACKSON LEE. So there was a crack in the resiliency, the start-up of getting back to where you were?

Dr. STEPHENS. Bigger than a crack.

Ms. JACKSON LEE. Okay.

Let me pose a question to you, Mr. Czerwinski. Your testimony clearly states that a resilience-based approach to disruptions, including intentional human-made attacks, is a company's best interests. How broadly practiced is such an approach within the private sector? How can it be promoted?

As Colonel Stephan is not a good piñata, I hope that you will give us a good critique of what we may do better in the Federal Government in answering the question.

Mr. CZERWINSKI. Understood. Thank you, Madam Chairwoman.

Is it the case that the entire private sector embraces this idea that resilience is in their economic interest? Likely not.

However, there is no doubt that the current efforts at the Department of Homeland Security to engage these separate 18 sectors to communicate to them the importance of understanding the threats that face them and the ways in which they can protect themselves is sinking in.

There is no question that there are some sectors that are absolutely more receptive to this than others. The financial services sector, let's say, or the I.T. sector, they understand their vulnerability and their criticality.

However, the next step beyond that is to be even more proactive to suggest that, in fact, there is a way we can bridge these different sectors to identify where these sectors are dependent upon one another. If we can do that, we can identify a different level of vulnerability that is no doubt part and parcel of the 21st century type of risk we are facing.

How that would be incentivized could be taken in a few different ways. One would be to provide a framework that allowed these private-sector participants to gain some different kind of treatment, let's say, when it interfaces with the government.

Customs and Border Protection does this now, where they work with multiple different sectors in their automated customs environment. They share information across different sectors. They, therefore, facilitate the flow of travel.

What that also provides them is the ability to see any sort of aberrations that may be threats themselves.

Ms. JACKSON LEE. Let me ask Mr. Raisch, does he have any examples through his research of companies who have done a good job at resilience? In your certification pilot or idea, does there need to be assessments—I hate to use the word punitive measures—but does there need to be a stronger assessment of whether or not there is a resilient plan?

Does there need to be some punitive measures, some fines assessed for those who don't have them? Is it that important?

You need to use as a backdrop Dr. Stephens, who indicated that pre-Katrina there were 11 hospitals. There are now four in New Orleans.

Mr. RAISCH. Clearly——

Ms. JACKSON LEE. Some of that is private, and some of that is public, and we understand the challenges. But just use it as a backdrop, that there was a problem with being resilient in New Orleans in the medical sector, and so if you would respond.

Mr. RAISCH. You bring in a very good point, assessment. I mean, the question, as I think someone else mentioned earlier, the issue is, what is preparedness or how much preparedness do we need?

It is a difficult situation to assess, just given the fact that many of us have different other operation responsibilities. Nonetheless, speaking to your issue of assessment, I think there is an opportunity, utilizing existing private-sector standards, to assess the level of preparedness.

These are standards that developed through common practice over the course of many years, input by corporations, professionals in this area. So I think the criteria exist currently to define effective preparedness.

The 9/11 Commission in particular recommended a particular standard in SK 1600 that was developed some—I guess early 1990s—as one of those standards. There are other ones out there, as well.

But what has been lacking in the past is a measurement methodology. That is what, essentially, the legislation that this Congress passed—I am sorry, last Congress passed in 2007, and the focus there specifically was on one of developing an assessment methodology that was built upon existing historical experience.

In the world of business, there is quality management. ISO 9000 is a type of certification manufacturers have gotten since the early, the mid-1980s, when quality was a problem in our manufacturing firms. We can leverage that, and I think that is what this program offers in the way of potential.

Relative to your other issues, I think you have specifically focused on, what can government do better, and particularly what can DHS do better?

I think the opportunity to be a convener—we don't have all the answers at this table. There are very learned individuals here, without doubt. I would like to say that there are pearls of wisdom that would roll out of each of our lips.

At the same time, I think the answer probably is resident out there. I think, just as this committee is convening experts, I think DHS could do a—increase its activities in convening, but convening with a specific focus, not only what should be done, but why should it be done, really getting Congress, congressional representation there, as well, to look at what both legislative issues, as well as market-based incentives are important.

We can't just look for these. We need, in some cases, to create them. By bringing together private sector, bringing together, I think, the congressional and legislative branch, and the executive branch, I think there is an opportunity, perhaps, to really define some, if you will, bottom-line rationale and develop it over time.

Ms. JACKSON LEE. So you don't think the certification should have a fine component to it?

Mr. RAISCH. Well, I think it is unrealistic at this point. Quite frankly, I don't think there is the political will to move this to a mandatory stage.

I think, quite frankly, though, there is a market-based punitive element to it, to the extent—let's give supply chains as an example. Many corporations out there right now, for their critical suppliers—we have financial services here as an example—they are regulated

already to bring their offices up and their operations up within 4 hours, many of them my primary market-maker.

At the same time, for them to do that, they need critical suppliers, in I.T., in telecom, in other elements of power generation. They are looking, in many cases, for tools, a measurement that would allow them to define whether or not those particular suppliers in their supply chain can be there for them when they are needed.

Now, if there is an effective measure out there and if their suppliers that they are currently using don't meet that measure, then you are going to see an economic impact, an economic punitive, if you will, element, that will suggest, "Jeez, if you are not prepared, I am going to go with this other entity over here that has validated its preparedness efforts."

This was done in the manufacturing industry, again, with quality management. It is done in environmental management. So I think there is good precedent there.

I think we should look for—the opportunity here is for government to be a convener and, if you will, to be a catalyst in creating and accessing this in the way of bottom-line incentives.

Ms. JACKSON LEE. Let me—I ask unanimous consent to move without a quorum—let me continue the other questioning. We are moving toward the floor for a vote.

Mr. Johnson, the financial services industry, because of Wall Street, I think, showed itself very much in tune with resilience. Is there one singular aspect of what happened during that time frame and what you have done since that you think is very important for us to have on the record as it relates to resilience and as you have seen it in the financial services industry?

Mr. JOHNSON. Thank you, Madam Chairman. I would say one thing that we have done and continue to do is test. I think if there is one lesson learned out of 9/11 is to—you can't test every scenario, but you can test.

I think that that is something that goes beyond financial services to, indeed, other sectors.

Ms. JACKSON LEE. So during the ongoing existence of your business, you are repeatedly testing your ability to be resilient?

Mr. JOHNSON. That is absolutely correct. Whether it was required by a regulation or not, it is done, because all of the financial services companies have, if you will, a motivation to ensure they can continue to operate.

If there is something that I think we have learned, testing does pay dividends. That would be my answer.

Ms. JACKSON LEE. Let me ask, Colonel Stephan, Secretary Stephan, to tell us what incentives DHS is providing to the public, to the public and private, private sector, to encourage more organizations to be resilient.

I know the documentation reports, but what is the engagement? What is the thought of having a chief that deals particularly with assessing risk, that companies may have within the DHS shop?

Colonel STEPHAN. Well, what we have done is—the infrastructure that we have identified to be most at-risk from various threat vectors across the country, they number about 2,800 to 3,000. We are very focused on——

Ms. JACKSON LEE. I didn't—what is 2,800 to 3,000?

Colonel STEPHAN. The infrastructures that we have determined to be the most at-risk across the country on a steady-state basis, lacking any specific——

Ms. JACKSON LEE. That is in the private sector?

Colonel STEPHAN. The private sector mostly, although there is——

Ms. JACKSON LEE. Focused on what incentives you are giving them to move toward resilience?

Colonel STEPHAN. Yes, ma'am. What we do is we have vulnerability assessment programs in concert with them, and we have buffer zone protection programs in concert with that. Where we do security planning, that facilitates interaction between the private-sector security folks, owners and operators, and local, State law enforcement and National Guard.

The incentive there is that, with DHS facilitation, we build a team of security and resiliency. Resiliency is embedded, built into the security plan template—so is cyber security, for that matter—rolling in there and facilitating the interaction and getting the private sector, local law enforcement, State law enforcement and the National Guard to pony up to the plate based upon this nucleus of critical individual facilities, assets, systems and networks that we work together to identify.

That is one example. The exercise piece, bringing people together very routinely, whether it is tabletop or full-scale boots on the ground activity, like we did last week, we have invited private-sector folks inside our National Infrastructure Coordinating Center for the first time last week, during our big national-level continuity of operations exercise, figuring out the resiliency piece, the security requirements, the information-sharing requirements, who needs what, based upon what type of disaster.

Last week, we dealt with the double-headed monster of a terrorism attack, as well as a major Category 4 hurricane hitting the national capital region.

Ms. JACKSON LEE. Mr. Secretary, let me ask that in writing if you will focus on—and I have heard the sort of give-and-take, and I think that we will ask staff to review closely the documents that you are submitting—but if you can give some particular corporate examples where DHS has interacted and, in the letter, writing of companies that are under a particular sector, showing the incentives and showing the give-and-take, and seeing the progress of resiliency being built under our present structure, I would appreciate it.

Colonel STEPHAN. We would be happy to do that.

Ms. JACKSON LEE. I want the record to be clear that Assistant Secretary Stephan is here, but he doesn't represent the wholeness of America, the wholeness of the Department of Homeland Security, though we appreciate his patriotism.

He is well able to engage in give-and-take to make things better. Is that my—and I hope that that clears the record.

Dr. Stephens, let me close by simply acknowledging your delegation with Melancon and Mr. Jefferson and others who have been diligent on working on New Orleans. We thank you.

We expect that you will be able to give us some very good insight. I would ask—I know your testimony has been put in the record—but I would ask to be able to follow up with you on the reason why, beyond the revenue stream, what the Federal Government has not done to ensure that the resiliency of your public health system, such as Charity Hospital, could not be in place 3 years after Hurricane Katrina, particularly the physical plant.

Maybe you could put that for me in writing. Would that be all right? I thank you so much.

As I do for all of the witnesses, I thank them very much for their testimony, valuable testimony. The members of the subcommittee may have additional questions for the witnesses, and we will ask you to respond expeditiously in writing to those questions.

Having no further business, the subcommittee stands adjourned. I will say thank each and every one of you for what has been an instructive, but, I am sorry, abbreviated hearing.

Thank you very much.

[Whereupon, at 3:50 p.m., the subcommittee was adjourned.]

○