

6 of 6 DOCUMENTS

Federal News Service

May 14, 2008 Wednesday

HEARING OF THE HOUSE HOMELAND SECURITY COMMITTEE'S  
TRANSPORTATION SECURITY AND INFRASTRUCTURE

**SUBCOMMITTEE;**

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

CHAired BY: REPRESENTATIVE SHEILA JACKSON-LEE (D-TX);

WITNESSES: COLONEL BOB STEPHAN, ASSISTANT SECRETARY  
FOR INFRASTRUCTURE PROTECTION, DEPARTMENT OF  
HOMELAND SECURITY; JONAH J. CZERWINSKI, SENIOR  
FELLOW FOR HOMELAND SECURITY, IBM GLOBAL

LEADERSHIP INITIATIVE; SHAWN JOHNSON, VICE CHAIRMAN  
FOR FINANCIAL SERVICES, SECTOR COORDINATING COUNCIL;

WILLIAM **RAISCH**, DIRECTOR, INTERNATIONAL CENTER FOR  
ENTERPRISE PREPAREDNESS, NEW YORK UNIVERSITY; DR.

KEVIN STEPHENS, DIRECTOR, HEALTH DEPARTMENT;

LOCATION: 311 CANNON HOUSE OFFICE BUILDING,  
WASHINGTON, D.C.

SECTION: CAPITOL HILL HEARING

LENGTH: 15533 words

HEARING OF THE HOUSE HOMELAND SECURITY COMMITTEE'S TRANSPORTATION SECURITY  
AND INFRASTRUCTURE **SUBCOMMITTEE** SUBJECT: PARTNERING WITH THE PRIVATE SECTOR TO  
SECURE CRITICAL INFRASTRUCTURE: HAS THE DEPARTMENT OF HOMELAND SECURITY  
ABANDONED THE RESILIENCE-BASED APPROACH? CHAired BY: REPRESENTATIVE SHEILA  
JACKSON-LEE (D-TX) WITNESSES: COLONEL BOB STEPHAN, ASSISTANT SECRETARY FOR  
INFRASTRUCTURE PROTECTION, DEPARTMENT OF HOMELAND SECURITY; JONAH J. CZERWINSKI,

HEARING OF THE HOUSE HOMELAND SECURITY COMMITTEE'S TRANSPORTATION SECURITY AND INFRASTRUCTURE SUBCOMMITTEE; SUBJECT: PARTNERING WITH THE PRIVATE SECTOR TO SECURE CRITICAL INFRASTRUCTURE: HAS THE DEPARTMENT OF HOMELAND SECURITY ABANDONED THE

SENIOR FELLOW FOR HOMELAND SECURITY, IBM GLOBAL LEADERSHIP INITIATIVE; SHAWN JOHNSON, VICE CHAIRMAN FOR FINANCIAL SERVICES, SECTOR COORDINATING COUNCIL; WILLIAM RAISCH, DIRECTOR, INTERNATIONAL CENTER FOR ENTERPRISE PREPAREDNESS, NEW YORK UNIVERSITY; DR. KEVIN STEPHENS, DIRECTOR, HEALTH DEPARTMENT LOCATION: 311 CANNON HOUSE OFFICE BUILDING, WASHINGTON, D.C. TIME: 2:00 P.M. EDT DATE: WEDNESDAY, MAY 14, 2008

REP. JACKSON LEE: Good afternoon, and 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 Reliance -- or 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'm 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 the 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 11th, most of the record 80 billion (dollars) in economic losses was survived by the private sector -- 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'm 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 for 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 a 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 over the last couple of years.

For example, Hurricane Katrina is a prime example of the lack of resiliency. Who know 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 have been done to major geographic areas, including the obliteration or elimination of whole cities? 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.

RESILIENCE-BASED APPROACH?; CHAIRED BY: REPRESENTATIVE SHEILA JACKSON-LEE (D-TX); WITNESSES: COLONEL BOB STEPHAN, ASSISTANT SECRETARY FOR INFRASTRUCTURE PROTECTION, DEPARTMENT OF HOMELAND SECURITY; JONAH J. CZERWINSKI, SENIOR FELLOW FOR HOMELAND

It is my belief that the department should utilize resilience as a means of which to encourage private owners and operators to secure the infrastructure for three reasons. It requires the provision of information that demonstrates to companies that there is an actual 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.

And, 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 attack likely do not generate such a profit. Third, a focus on protection and 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 a 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 objective. 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 are announcing supply change 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, 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 of our security.

Led by Chairman Thompson, we include language that calls 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 contemplative 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 the dialogue. I'm looking 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 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. And to do so, we need the involvement of the public and private sector.

Once again I'd like to thank everyone for their participation today, and I look forward to hearing from each of the witnesses. At this time I'd like to enter into the record the 2006 Homeland Security Advisory Council Report on Critical Infrastructure. Hearing no objection, so ordered.

SECURITY, IBM GLOBAL LEADERSHIP INITIATIVE; SHAWN JOHNSON, VICE CHAIRMAN FOR FINANCIAL SERVICES, SECTOR COORDINATING COUNCIL; WILLIAM RAISCH, DIRECTOR, INTERNATIONAL CENTER FOR ENTERPRISE PREPAREDNESS, NEW YORK UNIVERSITY; DR. KEVIN

The chair is now pleased to recognize the distinguished ranking member of the **subcommittee**, the gentleman from California, Mr. Lungren, for an opening statement.

REP. DANIEL E. LUNGREN (R-CA): Thank you very much, Chairwoman Jackson Lee, and 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 securing our critical infrastructure.

You probably know as well as anybody, those of you on the panel, that it's an enormous job because of the thousands of critical infrastructure assets we enjoy stretching from coast to coast and beyond. For sure, the 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've done in leading this effort on behalf of Homeland Security. And, also, I recall when you came and asked for a delay of its issuance until it met, by your judgment, the highest standards that you thought were required by identifying critical assets and interdependencies, coordinating risk-based protection programs and sharing information, and it 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, man-made or natural, because of commercial and economic benefits. And, I guess one of the questions we have is, how do we ensure that continues or, in those cases where it's 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's as important as anything else we do. If you don't have the proper information, it's very difficult to calculate what the threat is out there, and very difficult for you to respond to that threat. The government also provides grants while 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'm 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 and I look very much forward to the testimony from our witnesses.

And if I were still chairperson, I would -- (laughter) -- invite you to speak, but a funny thing happened on the way to the ballot box a couple years ago. (Laughter.) I would be happy to ask unanimous consent if I might include in the record the U.S. financial services sector exercise results of January 2008 and their pandemic flu exercise of 2007. I think this is a very good example of the kind of work that we wish to promote -- (off mike).

REP. JACKSON LEE: Without objection, so ordered.

STEPHENS, DIRECTOR, HEALTH DEPARTMENT; LOCATION: 311 CANNON HOUSE OFFICE BUILDING,  
WASHINGTON, D.C. Federal News Service May 14, 2008 Wednesday

REP. LUNGREN: And with that I would yield back the balance of my time.

REP. 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, and I might say -- I don't know if I want to say for the record because he looks very well to me, but we'll put it in the record so that he is covered. He is fighting off jet lag, but he has always been very gracious in his relationship with this committee and the Congress, and 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 a managing consultant in global business services at IBM, and a senior fellow for homeland security in IBM's global leadership initiative. First, we're 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 in 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](http://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 City Street, 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 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're 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

HEARING OF THE HOUSE HOMELAND SECURITY COMMITTEE'S TRANSPORTATION SECURITY AND INFRASTRUCTURE SUBCOMMITTEE; SUBJECT: PARTNERING WITH THE PRIVATE SECTOR TO SECURE CRITICAL INFRASTRUCTURE: HAS THE DEPARTMENT OF HOMELAND SECURITY ABANDONED THE

Katrina and knows firsthand the importance of health care infrastructure resiliency. Dr. Stephens serves as 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 come in 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. And 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. And so I welcome all of the witnesses, and without objection, the witnesses' full statements will be inserted in the record. And now I ask each witness to summarize his statement for five minutes, beginning with Assistant Secretary Stephan. You're recognized and welcome for five minutes.

MR. STEPHAN: Thank you, Madame Chairwoman and Ranking Member Lungren. I appreciate the opportunity to be before you today, and I also appreciate your ongoing leadership and focus in this very important subset of the Homeland Security overall mission area. I know you've heard previous testimony from some of my department counterparts, as well as key private sector stakeholders on this topic, and I have also hope from my heart that you have received a resounding no from them in response to the question that's titling this hearing, has the Department of the Homeland Security abandoned the resiliency-based approach?

Now this is not about abandoning a resiliency-based approach. The department fully embraces the concept of resiliency. It's not about protection vice resiliency; it's about both. It's about achieving an appropriate balance, Madame Chairwoman, as you have said in your opening statement, that's 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're saving American lives, limiting disruption to the economy and getting American society back on its feet as quickly as possible. That's what this debate is all about from my perspective.

Our focus on the nation's critical infrastructure includes actions to mitigate overall risk to asset systems, networks, functions and their interconnecting linkages resulting from any type of hazard, whether it be a terrorist attack, an attack on 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 the National Infrastructure Protection Plan, a wide range of activities, such as hardening facilities, building resiliency and redundancy, incorporating hazard resistance in a facility or system or network design, initiating active or passive counter measures, 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 to devise 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's 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've 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

RESILIENCE-BASED APPROACH?; CHAIRED BY: REPRESENTATIVE SHEILA JACKSON-LEE (D-TX); WITNESSES: COLONEL BOB STEPHAN, ASSISTANT SECRETARY FOR INFRASTRUCTURE PROTECTION, DEPARTMENT OF HOMELAND SECURITY; JONAH J. CZERWINSKI, SENIOR FELLOW FOR HOMELAND

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 example of the need to balance our concern about infrastructure restoration after an incident, with our ability to prevent the release of dangerous chemical substance into populated areas in the context of these sectors. After all, preventing the loss of American lives, innocent lives, must remain our number-one 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 of 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 risk 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 territorial 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 cyber-security or rapid response to minimize consequences.

Ma'am, I've shared 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, communication sector, 55 times, dams, 10 times, defense industrial base, 14 times, energy, 34 times, IT, 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've been working on for the past three years. In addition, I've 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've 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, pass 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. And finally, pandemic influenza across the 17 critical infrastructure sectors in the guide that we built with the private sector to highlight the needs 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've put into making sure we get this right and to achieve the balance that you spoke to at the beginning of the conversation.

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

REP. JACKSON LEE: I thank the assistant secretary. Without objection, we will put his entire testimony, including his documents, in the record. Thank you, again, and I now recognize Mr. Czerwinski to summarize his statement for five minutes. Welcome.

SECURITY, IBM GLOBAL LEADERSHIP INITIATIVE; SHAWN JOHNSON, VICE CHAIRMAN FOR FINANCIAL SERVICES, SECTOR COORDINATING COUNCIL; WILLIAM RAISCH, DIRECTOR, INTERNATIONAL CENTER FOR ENTERPRISE PREPAREDNESS, NEW YORK UNIVERSITY; DR. KEVIN

MR. CZERWINSKI: Maybe I should speak up or hit the talk button. Given the unique risks of the 21st century, resiliency is a necessary goal. And the balance you spoke of is key. I'm a senior fellow at the 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. And today I would like to touch upon three things.

First, resiliency and its definition, which can be an elusive concept meaning different things for 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.

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 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 coauthors and I outlined 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 improve performance and address risk. Strategic human capital requires leaders to employ emerging techniques for managing in a network environment, some of which are highlighted in my written statement. We also need to change how we use technology to seek efficiencies. By sharing 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 means by which to organize their efforts to address, the actual risks, costs and benefits that accrue to an organization in today's network environment. Our research shows that

STEPHENS, DIRECTOR, HEALTH DEPARTMENT; LOCATION: 311 CANNON HOUSE OFFICE BUILDING,  
WASHINGTON, D.C. Federal News Service May 14, 2008 Wednesday

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.

REP. JACKSON LEE: We thank you for your testimony, and I now recognize Mr. John to summarize his statement for five minutes.

MR. JOHNSON: Thank you, thank you Chairwoman Jackson-Lee, Ranking Member Lungren, and members of the committee. I'm 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 of the financial services sector, and in particular, the resilience-based related activities of the FSSCC. Though established at the request of the Department of the Treasury, the FSSCC is a private sector coalition working to improve the financial sector's resilience to terrorist attacks, man-made 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 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 Best Practices White Paper by the Federal Reserve, the OCC and SEC in 2003, addressing contingency planning and back-up facilities for clearing its own activities.

Implementation 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 financial services system.

The government participates in other less wealth formal activities, such as working with local public/private partnerships to sponsor resilience exercises which stimulate -- or simulate, excuse me, 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 the FSSCC, of which I'm 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've also worked to expand the GETS program, which provides access to priority telephone services during a crisis. We held a cyber security summit in February 2008 with private and public sector participation, and the FSSCC and FBIIC have since each launched new cyber security committees.

The FSSCC maintains relationships to help align academic research with real-world business seeds 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, PCIS, 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

HEARING OF THE HOUSE HOMELAND SECURITY COMMITTEE'S TRANSPORTATION SECURITY AND INFRASTRUCTURE SUBCOMMITTEE; SUBJECT: PARTNERING WITH THE PRIVATE SECTOR TO SECURE CRITICAL INFRASTRUCTURE: HAS THE DEPARTMENT OF HOMELAND SECURITY ABANDONED THE

FSSCC website.

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. 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 2,7000 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 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. Ninety nine percent of the participants found the exercise useful in assessing their organizations business planning needs. Ninety seven percent of the 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. 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, and I'll be pleased to answer any questions you have.

REP. JACKSON LEE: Mr. Johnson, thank you very much for your testimony. I now recognize Mr. **Raisch** to summarize his statement for five minutes.

MR. **RAISCH**: (Off mike) -- 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'm most honored to join you from the International Center for Enterprise Preparedness at New York University. As you mentioned, this center serves as a first academic center focused specifically on private sector resilience and preparedness. I am also most honored to serve as a private sector advisor to the 9/11 commission. More importantly, though, I'm here to reflect on a perspective garnered from 12 forms on this specific voluntary certification program held since this past fall involving over 550 private sector representatives and currently five different working groups with over 250 participants in the private sector.

Let me clearly state that there was substantial and growing interest and also concern in the private sector on this program. That being said, also, let me just say that it is my personal opinion that this single program has the potential for doing more to institutionalize or economically (indebt ?) 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; and further, it must actively and directly involve and engage the private sector in the development and ongoing implementation of the program itself.

RESILIENCE-BASED APPROACH?; CHAIRED BY: REPRESENTATIVE SHEILA JACKSON-LEE (D-TX); WITNESSES: COLONEL BOB STEPHAN, ASSISTANT SECRETARY FOR INFRASTRUCTURE PROTECTION, DEPARTMENT OF HOMELAND SECURITY; JONAH J. CZERWINSKI, SENIOR FELLOW FOR HOMELAND

Allow me to outline perhaps a couple of key considerations for this program going forward, and it -- 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, and as I said we've tried to reflect on this and really try to 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 for 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 certifications, 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 private sector and it evolved with private sector application for over two decades in many cases. There is also an existing accrediting body, ANAD, which has administered private sector certification for years as well. I'm 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 the 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 credit effective activities already in practice by each key sector. These sectors must be brought directly into the process. Fourthly, and finally, 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 the 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 and implementation of the program. Specific considerations and issues are identified in my written remarks on 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 & 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 an ongoing commitment by DHS to this program. It's 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

SECURITY, IBM GLOBAL LEADERSHIP INITIATIVE; SHAWN JOHNSON, VICE CHAIRMAN FOR FINANCIAL SERVICES, SECTOR COORDINATING COUNCIL; WILLIAM RAISCH, DIRECTOR, INTERNATIONAL CENTER FOR ENTERPRISE PREPAREDNESS, NEW YORK UNIVERSITY; DR. KEVIN

tool in cross-sector cooperation and assessment. A common reference platform, a "rosetta stone" of sorts, could aid in sharing best practices and cross-pollination 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 and protections for those proactive firms that undertake certification, perhaps including safe harbors and privilege or 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 anti-trust considerations, should also be addressed by Congress. I welcome your questions. Thank you.

REP. JACKSON LEE: (Off-mike) -- very much for your testimony, and I now recognize Dr. Stephens for five minutes. And Dr. Stephens, you may also summarize your statement, and be recognized for five minutes. Thank you

DR. STEPHENS: Thank you, Chairwoman Jackson-Lee, 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, and as you are all aware, it has faced many challenges in recovering and rebuilding after the world's -- and perhaps our worst natural and man-made disaster to occur in the United States of America.

Please know that I am speaking for our entire community and -- 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 continuous concerns about our progress and care of -- (audio break) -- our citizens, how we work diligently towards resolving longer term recovery challenges.

Thank you for -- (audio break) -- having this 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 which 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 in our city. We continue to struggle to rebuild the healthcare foundation and cover basic medical needs of 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 healthcare for the indigent and uninsured, and minimal medical surge capacity, even though we are ranked high in vulnerability in terms of terrorism and natural disasters.

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 successful solutions. One of our challenges is in the recovery and building resilience that plagues our healthcare providers is that the duality that they place as victims as well as respondents in a critically needed system. It is quite difficult -- (audio break) -- both of these roles simultaneously. Many of our providers have 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 reopen their facilities, and those that remain have a drastically reduced number of in-patient beds. This reduced capacity and

STEPHENS, DIRECTOR, HEALTH DEPARTMENT; LOCATION: 311 CANNON HOUSE OFFICE BUILDING,  
WASHINGTON, D.C. Federal News Service May 14, 2008 Wednesday

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 further damage of an already decimated healthcare system.

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

Many of our private sector hospitals realize that rather quickly following Hurricane Katrina that financial risks were tremendous. These institutions faced higher labor costs, higher insurance costs, higher provider costs, higher uninsured numbers, and higher construction costs. It is evident that if they open -- reopen, that they will be likely to lose millions of dollars. Hence, four of our regional healthcare facilities have decided not to reopen.

As mentioned earlier, providers in providing care in an increasing indigent and uninsured population due to additional cases of job losses 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 hospital system immediately after the hurricane, private hospitals were forced to assume the care of the uninsured. Such compensation for these services were provided by the state at a later date, however, but according to many COOs, it was 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 healthcare information at the time of a disaster. Entrepreneurs have also identified this and are flooding the market with various forms of mobile personal data, all kinds of systems, while many healthcare providers and (associates ?) have agreed to the critical fields and a continuity of care record. A federally standardized approach is warranted. One must ask, why can we access our email accounts, banking information and other critical data while we are abroad, but no such means for accessing our medical data exists.

Number two, for our providers -- some of our actions -- views that were performed were performed after Hurricane Katrina responded cited a need for mechanisms where providers can easily access across state boundaries in a response to a disaster. An avenue for expediting medical licensure and certification needs to be in place to facilitate the credentialing and responding healthcare 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 created the emergency system by advanced registration of volunteer and health professionals in response to 9/11, we need more emphasis on this linking various states, because this is primarily a state run program. We need a national registry of providers.

And for the hospitals, the healthcare community is pleading for a more reliable and predictable reimbursement mechanism for providers and hospitals that respond to a disaster, as declared by our new president. The private sector must also 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 occurring after a

HEARING OF THE HOUSE HOMELAND SECURITY COMMITTEE'S TRANSPORTATION SECURITY AND INFRASTRUCTURE SUBCOMMITTEE; SUBJECT: PARTNERING WITH THE PRIVATE SECTOR TO SECURE CRITICAL INFRASTRUCTURE: HAS THE DEPARTMENT OF HOMELAND SECURITY ABANDONED THE

disaster. For example, Medicaid payments should be made portable from the time of a declared disaster so that health providers in another state --

REP. JACKSON LEE: Dr. Stephens, if you could -- I don't know how much more you have.

DR. STEPHENS: That's it.

REP. JACKSON LEE: If you could summarize for us please --

DR. STEPHENS: Yeah.

REP. JACKSON LEE: Thank you.

DR. STEPHENS: The other states will basically full-facing credit to the whole state Medicaid insurance cards.

And finally, we do acknowledge that we have a whole lot of initiatives organized and authorized by Congress and the ESAI and the Metropolitan Response System, and they are under funded and we will suggest that there 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.

REP. JACKSON LEE: I thank you very much for your testimony. I thank all the witnesses for their testimony, and I remind each member that he or she will have five minutes to question the panel. I now recognize myself for five minutes.

Assistant Secretary Stephan, we hear the number 85 percent over and over again of the critical infrastructures owned and operated by the private sector. Among that 85 percent, with what percentage does the Department continuously engage for critical infrastructure security purposes, and because many of these assets are not regulated for security purposes, what is the business case the Department makes to these entities to secure the assets? What are the carrots you use to get them to do the right thing? And do you encourage the private sector to be resilient and be able to bounce back to effective operations, and how do you do that?

DR. STEPHAN: Yes, ma'am. To answer your first question, I do not have an exact percentage for you, though 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, IT, transportation, you name it. We have a sustained governance mechanism that allows very frequent meetings between our different entities, as well as in 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're monitoring today, ongoing activities and relationships.

Resiliency is built in as part of our organizing framework in terms of national level documents that we've built in voluntary partnership with the private sector over the past three 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 this sector, we do everything we can to develop tierline (ph) 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've got a special team of analysts in my shop and Charlie Allen's (sp) shop that work on lessons learned from abroad. If the terrorists aren't attacking hotels and discos and transport systems here, they're certainly doing it abroad almost every day somewhere, Iraq, Afghanistan, Indonesia, Jordan,

RESILIENCE-BASED APPROACH?; CHAIRED BY: REPRESENTATIVE SHEILA JACKSON-LEE (D-TX); WITNESSES: COLONEL BOB STEPHAN, ASSISTANT SECRETARY FOR INFRASTRUCTURE PROTECTION, DEPARTMENT OF HOMELAND SECURITY; JONAH J. CZERWINSKI, SENIOR FELLOW FOR HOMELAND

Egypt, you name it. There they are. We're capturing those lessons learned, learning the techniques and procedures, and exporting that information across our private sector information network.

REP. JACKSON LEE: Let me quickly ask another question. You've submitted a lot of documents. Do you have an internal white paper or managerial directives dealing with infrastructure protection that define resiliency and how it's going to be implemented? And if you have those, we'd like to have those submitted to the committee.

MR. 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've provided, brought with me today to submit to the committee.

REP. JACKSON LEE: Do you have how it can be implemented? Is that --

MR. STEPHAN: Ma'am, it's all part and parcel of the framework. And 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 who would like to drive a wedge and cause us to make a choice between protection, prevention, and a response and recovery side or other 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's how do we combine the two imperatives? How do we blend them?

And on the prevention and protect 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're not for that risk-based approach to the up front components combined with a capability to absorb a strike and respond adequately. That's what this nation is all about.

REP. JACKSON LEE: Well, let me get Mr. Czerwinski, Mr. Johnson, Mr. **Raisch** to respond to that. Mr. Czerwinski?

MR. CZERWINSKI: Thank you, Madam Chairwoman. The 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 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.

And 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 this different kind of resiliencies evolve. The redundancy is a part of this, but the federal government has to embrace -- but the redundancy is not the sort that the private sector is going to be too enthusiastic about it. So there are still some opportunity to -- (off mike).

REP. JACKSON LEE: And you think that the federal government can do a better job?

MR. CZERWINSKI: Well, I'm an American citizen. I always think the American government can do a better job. But 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 --

REP. 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. And 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'd like to see what your thoughts are please. Mr. Johnson?

SECURITY, IBM GLOBAL LEADERSHIP INITIATIVE; SHAWN JOHNSON, VICE CHAIRMAN FOR FINANCIAL SERVICES, SECTOR COORDINATING COUNCIL; WILLIAM RAISCH, DIRECTOR, INTERNATIONAL CENTER FOR ENTERPRISE PREPAREDNESS, NEW YORK UNIVERSITY; DR. KEVIN

MR. JOHNSON: Well, 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 efficiently 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 differently 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 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.

REP. JACKSON LEE: Is that the industry spending money?

MR. JOHNSON: That is the industry spending money.

REP. JACKSON LEE: And 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, and 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.

REP. 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.

REP. JACKSON LEE: Well, let me do this. I mean, a document that's already been submitted to the record is fine. The question is whether there is interaction that focuses on resilience. And let me yield to Mr. **Raisch** -- and I thank you for your answer -- so I can yield to the distinguished ranking member from California.

MR. **RAISCH**: Thank you, chairwoman. A few brief comments. I would say firstly I don't think it's an either/or, prevention versus resiliency. This is a continuum, and --

REP. JACKSON LEE: We agree on that.

MR. **RAISCH**: Got that.

REP. JACKSON LEE: But we want to know whether the federal government can do better. That's what we'd like to hear.

MR. **RAISCH**: And certainly I would think the assistant secretary would agree. We can always --

REP. JACKSON LEE: And the secretary is not the singular representation --

MR. **RAISCH**: Yes.

REP. JACKSON LEE: -- of the federal government, so --

MR. **RAISCH**: Certainly.

STEPHENS, DIRECTOR, HEALTH DEPARTMENT; LOCATION: 311 CANNON HOUSE OFFICE BUILDING,  
WASHINGTON, D.C. Federal News Service May 14, 2008 Wednesday

REP. JACKSON LEE: -- I know you're 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 be more prepared. Quite frankly, that's 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. And as such, I think DHS and other elements of government, Congress included, can help clarify some of the business case incentives, develop perhaps new ones.

As I mentioned in my testimony before, I think the 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've 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. And if you can't acknowledge it or measure it, you can't reward it. So I think there's a real opportunity in moving forward this voluntary certification program, particularly with an emphasis towards economic value to business.

REP. JACKSON LEE: Thank you. I will -- Dr. Stephens, I'm going to hold my questions for you, and I yield to the distinguished gentleman for his time of questioning from California

REP. LUNGREN: Thank you very much. I think the panel is to be commended for resisting the temptation to treat Colonel Stephan as a pinata here. Colonel, I happen to think that you've done a very good job and the Department has done a good job in launching this effort, and that's what we've done. We've launched the effort. There's still remains a lot to be done.

And 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, and it seems to me that's 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**: Yes.

REP. LUNGREN: -- Mr. **Raisch** and Mr. Czerwinski. Let's presume the government -- the answer is not going to be in a lot more government money.

Let's just set that aside because that's an easy one to say -- well, we'll give you more grants, we'll 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, 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's more than resilience. It's also protection and prevention from terrorist attack or natural disaster.

MR. CZERWINSKI: Alright, well -- yeah, I'll go first. And thank you for that question. This gets to the real critical point, which is how does this, you know, issue become portable across different sectors? What we tried to look at actually was the cargo container, flow of cargo and container traffic across the (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's going on from end-to-end for a container cargo shipper. That is obviously useful from a regular bottom line perspective because it gives you the understanding of where disruptions exist, where inefficiencies are.

HEARING OF THE HOUSE HOMELAND SECURITY COMMITTEE'S TRANSPORTATION SECURITY AND INFRASTRUCTURE SUBCOMMITTEE; SUBJECT: PARTNERING WITH THE PRIVATE SECTOR TO SECURE CRITICAL INFRASTRUCTURE: HAS THE DEPARTMENT OF HOMELAND SECURITY ABANDONED THE

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 decision maker to say this disruption is actually unique. This is not a situation where we're looking at a derailment of a certain cargo, but we're looking at something completely new. Without the ability to have that visibility, that decision maker wouldn't be able to say we need to react differently, or we need to reroute 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.

REP. 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're organized as individual organizations, and as such, that's their focus primarily. I think government can bring a wider perspective. I think we've 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 of -- diversity, whether 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's a lot of good learning that's 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. And I think this -- again, getting back to the certification program, I think that offers a tremendous opportunity to do so.

So I think facilitating cross pollination across various sectors who 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're all very much integrated. And I think that is very much a governmental role in that respect and one that I think provides assistance.

And 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's some good things being done now on ready.gov, but I think we can move forward and have a truly robust resource from a electronic or web- based environment that facilitates business preparedness across the nation.

REP. 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've factored in and factored out educational -- 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 resilience. And in New Orleans particularly we are so busy trying to just mind 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.

RESILIENCE-BASED APPROACH?; CHAIRED BY: REPRESENTATIVE SHEILA JACKSON-LEE (D-TX); WITNESSES: COLONEL BOB STEPHAN, ASSISTANT SECRETARY FOR INFRASTRUCTURE PROTECTION, DEPARTMENT OF HOMELAND SECURITY; JONAH J. CZERWINSKI, SENIOR FELLOW FOR HOMELAND

REP. LUNGREN: See, I recall over about a 25 or 30-year period of time -- federal government decision making drove hospitals to be more, quote, unquote, "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. And I've seen it in communities across America. We prided ourselves on making our healthcare system more efficient, and one of the indices was, hey, we have fewer beds sitting out there. That's great unless you need the beds.

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

DR. STEPHENS: And your point is highlighted with the mental health beds. 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's private and public. So that point is well taken.

REP. LUNGREN: (Off mike.)

REP. JACKSON LEE: I thank the gentleman and yield myself an additional five 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.

REP. JACKSON LEE: And what do you have now?

DR. STEPHENS: Open, we have four.

REP. JACKSON LEE: Do you have a public Charity Hospital open?

DR. STEPHENS: Yes, we do. We have University Hospital, which is our charity hospital.

REP. 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 hospital -- Charity Hospital has had two -- hospital -- University -- in the old Charity that -- as we knew it.

REP. JACKSON LEE: And it was open prior to --

DR. STEPHENS: Yes, they both were open.

REP. JACKSON LEE: -- Katrina.

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

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

DR. STEPHENS: University -- University Hospital.

REP. JACKSON LEE: Has how many beds?

DR. STEPHENS: Two hundred.

REP. JACKSON LEE: How many did Charity have?

SECURITY, IBM GLOBAL LEADERSHIP INITIATIVE; SHAWN JOHNSON, VICE CHAIRMAN FOR FINANCIAL SERVICES, SECTOR COORDINATING COUNCIL; WILLIAM RAISCH, DIRECTOR, INTERNATIONAL CENTER FOR ENTERPRISE PREPAREDNESS, NEW YORK UNIVERSITY; DR. KEVIN

DR. STEPHENS: Totally they had 539, as I recall.

REP. JACKSON LEE: Is that building still standing?

DR. STEPHENS: It's still standing.

REP. JACKSON LEE: 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's correct.

REP. JACKSON LEE: And you now have four.

DR. STEPHENS: Correct.

REP. 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 Orleans -- people from New Orleans. Is that correct?

DR. STEPHENS: That's correct.

REP. 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 --

(Cross talk.)

DR. STEPHENS: -- to go from beds, we had 2,258 beds available in New Orleans before Katrina, and now we have less than 1,000 available.

REP. JACKSON LEE: And there was a MASH unit that was in, I believe, the Hyatt. Has that been closed?

DR. STEPHENS: Yes, it has, ma'am.

REP. JACKSON LEE: And where do those patients now go?

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

REP. JACKSON LEE: And 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.

REP. JACKSON LEE: So what could've been -- and you have made your appropriate statements and 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've 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 healthcare system in New Orleans fall after Hurricane Katrina? What was missing --

DR. STEPHENS: I think --

REP. JACKSON LEE: -- to put you in near capacity?

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

STEPHENS, DIRECTOR, HEALTH DEPARTMENT; LOCATION: 311 CANNON HOUSE OFFICE BUILDING,  
WASHINGTON, D.C. Federal News Service May 14, 2008 Wednesday

We had several hospitals that opened up, but we couldn't tell them for the uninsured -- when our Charity Hospital system closed and 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 EMTALA laws require that if somebody shows up in the 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 are -- I think I heard like \$135 million was lost last year amongst five hospitals that were open. And so without a predictable, reliable source of income, the private sector said they're for profit. They have to show --

REP. JACKSON LEE: So there is an aspect to resiliency that deals with a revenue stream.

DR. STEPHENS: Absolutely.

REP. JACKSON LEE: And 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.

REP. JACKSON LEE: What was the difficulty in opening -- what was the missing resiliency that would allow you to open the other Charity Hospital of 539 beds?

DR. STEPHENS: Well, the other Charity Hospital, as I understand it, had -- from the flooding, they had structural integrity problems and, in fact, there's a group now, architectural firm, that's looking at that facility to see what impediments are preventing this one from being open or not. It was a old facility, grant you, and it had many problems, but I'm not real sure. That's a very hot potato, if you will.

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

DR. STEPHENS: That's correct.

REP. JACKSON LEE: Okay, so there was a crack in the resiliency, the start-up of getting back to where you were.

DR. STEPHENS: It's bigger than a crack.

REP. 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 in a company's best interests. How broadly practiced is such an approach within the private sector, and how can it be promoted? And as Mr. -- Colonel Stephan is not a good pinata, 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 interests? 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.

And there's 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 IT 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's a way we can bridge these different sectors to identify where these sectors are dependent upon one another. And 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're facing.

HEARING OF THE HOUSE HOMELAND SECURITY COMMITTEE'S TRANSPORTATION SECURITY AND INFRASTRUCTURE SUBCOMMITTEE; SUBJECT: PARTNERING WITH THE PRIVATE SECTOR TO SECURE CRITICAL INFRASTRUCTURE: HAS THE DEPARTMENT OF HOMELAND SECURITY ABANDONED THE

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 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, and 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.

REP. 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, and in your certification pilot or idea does there need to be -- assessments. I hate to use the word punitive measures, but there needs to be a stronger assessment of whether or not there's a resilient plan, and does there need to be some punitive measure, some fines assessed for those who don't have them? Is it that important? And 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 --

REP. JACKSON LEE: And some of that's private and some of it 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'd respond --

MR. **RAISCH**: And you bring out a very good point. Assessment -- the question is -- I think someone else mentioned earlier -- the issue is, you know, what is preparedness, or how much preparedness do we need? And it's a typical situation to assess just given the fact that many of us have different -- other operational 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. And 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 exists currently to define effective preparedness. The 9-11 Commission in particular recommended a particular standard, NFPA 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, and that's what -- essentially the legislation that this Congress passed -- I'm 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's quality management. ISO 9,000 is a type of certification manufacturers have gotten since the early -- the mid '80s when quality was a problem at our manufacturing firms. We can leverage that, and I think that's what this program offers in the way of potential.

Relative to your other issues, I think you had specifically focused on what can government do better -- protect the -- 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'd 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, and 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 of what should be done, but why should it be done, really getting Congress -- congressional representation there as well -- to look at 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. And by bringing together the private sector, bringing together I think the congressional legislative branch and the executive branch, I think there's an opportunity perhaps to really define some, if you will, bottom line rationale and develop it over time.

REP. JACKSON LEE: And you don't think the certification should have a fine component to it?

RESILIENCE-BASED APPROACH?; CHAIRED BY: REPRESENTATIVE SHEILA JACKSON-LEE (D-TX); WITNESSES: COLONEL BOB STEPHAN, ASSISTANT SECRETARY FOR INFRASTRUCTURE PROTECTION, DEPARTMENT OF HOMELAND SECURITY; JONAH J. CZERWINSKI, SENIOR FELLOW FOR HOMELAND

MR. RAISCH: Well, I think it's unrealistic at this point. Quite frankly, I don't think there's 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 the critical suppliers. We have financial services here as an example. They are regulated already to bring their offices up and their operations up within four hours, many of them primary market maker.

And at the same time, for them to do that, they need critical suppliers in IT, in telecom, in other elements of power generation. They're 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're needed. Now, if there's an effective measure out there, and if their suppliers that they are currently using don't meet that measure, then you're going to see an economic impact -- an economic punitive, if you will, element -- that will suggest -- geez, if you're not prepared, I'm going to go with this other entity over here that has validated its preparedness efforts.

And this was done in the manufacturing industry, again, with quality management. It's done in environmental management. So I think there's good precedent there, and I think we should look for the -- 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.

REP. JACKSON LEE: Let me ask unanimous consent to move without a quorum. Let me continue the other questioning, and we are moving towards 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 timeframe and what you've done since that you think is very important for us to have on the record as it relates to resilience and as you've 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. And I think that that is something that goes beyond financial services to indeed other services.

REP. JACKSON LEE: So during the ongoing existence of your business, you're repeatedly testing your ability to be resilient.

MR. JOHNSON: That is absolutely correct. And 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. And if there is something that I think we've learned, testing does pay dividends. And that would be my answer.

REP. JACKSON LEE: Let me ask Colonel Stephan -- Secretary Stephan to tell us what incentives that DHS is providing to the public -- to the public and private -- the private sector -- to encourage more organizations to be resilient? I know the documentation reports, but what is the engagement? What's the thought of having a chief that deals particularly with assessing risk that companies may have within the DHS shop.

MR. STEPHAN: Yes, well, what we've done is -- the infrastructure that we've identified to be most at risk from various threat factors across the country -- they number about 2,800 to 3,000. We're very focused --

REP. JACKSON LEE: What is 2,800 to 3,000?

MR. STEPHAN: The infrastructures that we've determined to be the most at risk across the country on a steady state basis lacking any specific --

REP. JACKSON LEE: And that's in the private sector?

SECURITY, IBM GLOBAL LEADERSHIP INITIATIVE; SHAWN JOHNSON, VICE CHAIRMAN FOR FINANCIAL SERVICES, SECTOR COORDINATING COUNCIL; WILLIAM RAISCH, DIRECTOR, INTERNATIONAL CENTER FOR ENTERPRISE PREPAREDNESS, NEW YORK UNIVERSITY; DR. KEVIN

MR. STEPHAN: Private sector mostly.

REP. JACKSON LEE: And focus on what incentives you're giving them to move toward resilience.

MR. 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 them 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 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, asset systems and networks that we work together to identify. That's one example.

The exercise piece, bringing people together very routinely, whether it's tabletop or full-scale boots on the ground activity, like we did last week. We've 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 a double-headed monster of a terrorism attack, as well as a major Category 4 hurricane hitting the National Capital Region.

REP. JACKSON LEE: Mr. Secretary, let me ask that in writing if you will focus on -- and I've heard the sort of give and take, and I think that we will ask staff to review closely the documents that you're 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.

MR. STEPHAN: We'd be happy to do that.

REP. JACKSON LEE: And 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, and he is well able to engage in give and take to make things better. And I hope that that clears the record.

Dr. Stephens, let me close by simply acknowledging your delegation with Melanson and Mr. Jefferson and others who have been diligent on working on New Orleans, and we thank you. We expect that you will be able to give us some very good insight. And I would ask -- I know your testimony's been put in the record, but I'd 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 three years after Hurricane Katrina, particularly the physical plant. Maybe you could put that for me in writing. Would that be alright?

And 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, and I will say thank each and every one of you for what has been an instructive, but I'm sorry, abbreviated hearing. Thank you very much.

**LOAD-DATE:** May 17, 2008

**LANGUAGE:** ENGLISH

**PUBLICATION-TYPE:** Transcript

STEPHENS, DIRECTOR, HEALTH DEPARTMENT; LOCATION: 311 CANNON HOUSE OFFICE BUILDING,  
WASHINGTON, D.C. Federal News Service May 14, 2008 Wednesday

Copyright 2008 Federal News Service, Inc.  
All Rights Reserved