S. Hrg. 110–317

PRIVATE SECTOR PREPAREDNESS

HEARING

BEFORE THE

AD HOC SUBCOMMITTEE ON STATE, LOCAL, AND PRIVATE, SECTOR PREPAREDNESS AND INTEGRATION

OF THE

COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS UNITED STATES SENATE

ONE HUNDRED TENTH CONGRESS

FIRST SESSION

JUNE 21, 2007

PART I: DEFINING THE PROBLEM AND PROPOSING SOLUTIONS

JULY 12, 2007

PART II: PROTECTING OUR CRITICAL INFRASTRUCTURE

Available via http://www.access.gpo.gov/congress/senate

Printed for the use of the Committee on Homeland Security and Governmental Affairs

U.S. GOVERNMENT PRINTING OFFICE

36–615 PDF WASHINGTON : 2008

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

COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS

JOSEPH I. LIEBERMAN, Connecticut, *Chairman*

CARL LEVIN, Michigan
DANIEL K. AKAKA, Hawaii
THOMAS R. CARPER, Delaware
MARK L. PRYOR, Arkansas
MARY L. LANDRIEU, Louisiana
BARACK OBAMA, Illinois
CLAIRE McCASKILL, Missouri
JON TESTER, Montana

SUSAN M. COLLINS, Maine
TED STEVENS, Alaska
GEORGE V. VOINOVICH, Ohio
NORM COLEMAN, Minnesota
TOM COBURN, Oklahoma
PETE V. DOMENICI, New Mexico
JOHN WARNER, Virginia
JOHN E. SUNUNU, New Hampshire

MICHAEL L. ALEXANDER, *Staff Director*
BRANDON L. MILHORN, *Minority Staff Director and Chief Counsel*
TRINA DRIESSNACK TYRER, *Chief Clerk*

AD HOC SUBCOMMITTEE ON STATE, LOCAL, AND PRIVATE SECTOR PREPAREDNESS AND INTEGRATION

MARK L. PRYOR, Arkansas, *Chairman*

DANIEL K. AKAKA, Hawaii
MARY L. LANDRIEU, Louisiana
BARACK OBAMA, Illinois
CLAIRE MCCASKILL, Missouri
JON TESTER, Montana

JOHN E. SUNUNU, New Hampshire
GEORGE V. VOINOVICH, Ohio
NORM COLEMAN, Minnesota
PETE V. DOMENICI, New Mexico
JOHN WARNER, Virginia

KRISTIN SHARP, *Staff Director*
MICHAEL MCBRIDE, *Minority Staff Director*
AMANDA FOX, *Chief Clerk*

CONTENTS

Opening statements: Page
Senator Pryor 1
Senator Akaka 2
Senator Sununu 19

WITNESSES

THURSDAY, JUNE 21, 2007

Alfonso Martinez-Fonts, Jr., Assistant Secretary, Private Sector Office, U.S. Department of Homeland Security 4
Marko Bourne, Director of Policy and Program Analysis, Federal Emergency Management Administration, U.S. Department of Homeland Security 7
F. Duane Ackerman, Former Chairman and CEO, BellSouth Corporation, Business Response Task Force, Business Executives for National Security (BENS) 10
Hon. John Breaux, Former U.S. Senator from the State of Louisiana, Co-Chair, Business Response Task Force, Business Executives for National Security (BENS) 12
Richard Andrews, Ph.D., Senior Advisor for Homeland Security, National Center for Crisis and Continuity Coordination 15

THURSDAY, JULY 12, 2007

Colonel Robert B. Stephan, Assistant Secretary for Infrastructure Protection, U.S. Department of Homeland Security 37
Eileen Regan Larence, Director, Homeland Security and Justice Issues, U.S. Government Accountability Office 42
Lieutenant Colonel Kenneth C. Watson, (Retired), Vice Chairman, Partnership for Critical Infrastructure Security, Inc., and Senior Manager, Critical Infrastructure Assurance Group, Cisco Systems, Inc. 45

ALPHABETICAL LIST OF WITNESSES

Ackerman, F. Duane:
Testimony 10
Prepared statement 85
Andrews, Richard, Ph.D.:
Testimony 15
Prepared statement 97
Bourne, Marko:
Testimony 7
Prepared statement 72
Breaux, Hon. John:
Testimony 12
Prepared statement 91
Larence, Eileen Regan:
Testimony 42
Prepared statement 115
Martinez-Fonts, Alfonso, Jr.:
Testimony 4
Prepared statement 59
Stephan, Colonel Robert B.:
Testimony 37
Prepared statement 104

Page

Watson, Lieutenant Colonel Kenneth C.:
Testimony 45
Prepared statement 140

APPENDIX

"Getting Down to Business: An Action Plan for Public-Private Disaster Response Coordination," The Report of the Business Response Task Force, January 2007 148
Responses to Questions for the Record from:
Mr. Bourne 208
Mr. Ackerman 223

PART I: DEFINING THE PROBLEM AND PROPOSING SOLUTIONS

THURSDAY, JUNE 21, 2007

U.S. SENATE,
AD HOC SUBCOMMITTEE ON STATE, LOCAL, AND
PRIVATE SECTOR PREPAREDNESS AND INTEGRATION,
OF THE COMMITTEE ON HOMELAND SECURITY
AND GOVERNMENTAL AFFAIRS,
Washington, DC.

The Subcommittee met, pursuant to notice, at 2:06 p.m., in Room SD–342, Dirksen Senate Office Building, Hon. Mark Pryor, Chairman of the Subcommittee, presiding.

Present: Senators Pryor, Akaka, and Sununu.

OPENING STATEMENT OF SENATOR PRYOR

Senator PRYOR. Let me convene our inaugural meeting of the Subcommittee and welcome my colleagues. Senator Sununu is on his way. I want to thank the panel for being here today.

This is a new Subcommittee of the Homeland Security and Governmental Affairs Committee. It was created with the start of this Congress to focus attention on the coordination between the American business community and the government in disaster preparedness and response.

When you look at Hurricane Katrina, you see that some Federal agencies were prepared—for example, the National Guard and the Coast Guard—while others weren't. We all remember stories about ice trucks driving around the country or people overpaying for things when they could have been given for free. We are not here to revisit all of that today, but we really want to learn lessons from the private sector to get ideas on how the government can be more prepared and also how we, as a Nation, can be more prepared for disasters.

Hurricane Katrina was one of the most horrific natural disasters in our Nation's history, but one of the good news stories that came out of it was that there were 254 different companies contributing $1 million or more in connection with Hurricane Katrina. Wal-Mart, one of my home State companies, provided $13.5 million to employees affected by the storm, $17 million to non-employee disaster relief funds, and almost $4 million in merchandise and in-kind donations. But like I said, there were 254 companies that made over $1 million of contributions in one way or the other, so the American business community has a lot that it can be proud of.

And we have seen for years good working relationships in the business community with the government in various ways. One example is the Highway Watch Program, basically was started in the 1990s when law enforcement agencies approached the trucking industry to help report road hazards, to be the eyes and ears out there on the roads when the law enforcement agencies weren't around. And now, the American Trucking Association and Department of Homeland Security together train nearly every trucker on the road to watch for suspicious terrorist activity.

So we know that public and private partnerships work. We know there is a great track record when we work together and I am very pleased to mention that in June 2006, a non-partisan business executive group, the Business Executives for the National Security (BENS), formed a task force to specifically address the integration of public and private preparedness. They came out with a report, which I think we all have copies of, called "Getting Down to Business: An Action Plan for Public-Private Disaster Response Coordination."

There is a lot in this report, but basically, there are three main findings.

One, is that the private sector must be systematically integrated into national preparedness and response efforts. Two, is that commercial supply chains can provide a wider range of goods and services than government entities. And three, regulatory and credentialing improvements should be made, and these recommendations have sparked a lot of interest and discussion about public-private partnerships, which I think is very healthy.

The hearing today will examine the current state of public-private collaboration. Our witnesses will talk about how they view the current state of public-private partnerships. It is my understanding that DHS and FEMA have embraced many of the recommendations and have taken some initial steps on that. The Subcommittee would love to have a progress report on how that is going and how you see that unfolding over the next few months.

And I also hope that today's review will help us determine whether the government and the private sector have the tools they need to continue to improve our response capabilities.

Senator Akaka, would you like to make an opening statement? Go ahead.

OPENING STATEMENT OF SENATOR AKAKA

Senator AKAKA. Thank you very much, Mr. Chairman. I want to join you in welcoming our witnesses, all of you here, to this hearing. Also, I want to note my good friend and colleague John Breaux. John, will you please give my aloha to Lois. We have had many good years together here in the House and in the Senate.

I want to thank you, Mr. Chairman, for organizing this important hearing to begin discussions on how the public and private sectors can collaborate more effectively to prepare for and respond to natural and manmade disasters.

Despite the catastrophe of September 11, 2001, and the renewed focus on disaster planning in its aftermath, Hurricane Katrina starkly demonstrated that much more must be done at all levels

of the government and the private sector to plan and prepare for disasters. We need innovative approaches to incident management.

The government cannot succeed without forging a partnership with the private sector. The private sector owns approximately 85 percent of our Nation's critical infrastructure. The private sector has the expertise and the resources to play a leading role at every stage of response and recovery. With improved disaster planning and response, cooperation between the two will result in a reduction in the loss of life and property, which is the overall goal of emergency management.

Because of its unique geography, my home State of Hawaii is at risk of many natural catastrophes. Just last year, an earthquake measuring 6.7 on the Richter Scale caused extensive property damage on the big Island of Hawaii as well as on Maui. I am acutely aware of the need for an all-hazards approach to disaster preparedness and response, and I believe that in order to be effective, this approach must include public, private, and non-profit cooperation in the development of guidance, standards, plans, and solutions.

I hope today's witnesses will address their agency and organizational efforts to ensure that disaster preparedness and emergency response planning is inclusive of all stakeholders affected by disasters.

I also was interested in the conclusion of the BENS task force that the government should do a better job of tapping commercial supply chains to get relief to those in need after a disaster. This type of collaboration is especially important to Hawaii. Because of our separation from the mainland, it takes much longer for relief to be sent by other States to reach those in need.

My Subcommittee on Oversight of Government Management, which recently held a hearing on procurement at DHS, has taken a keen interest in government procurement practices. It is essential that DHS work closely with FEMA to put contracts into place with the private sector that can ensure that when disasters strike, we have the resources necessary to respond and that we can move supplies quickly to where they are needed. I look forward to hearing more about this topic. Dialogues like this are an important part of ensuring that when the next major disaster strikes, we will have systems in place to provide needed relief in a way that is swift, comprehensive, coordinated, and cost-effective for the American people.

Again, Mr. Chairman, I thank you for holding this hearing. I look forward to learning more about the private sector preparedness initiatives that are being considered and implemented. Thank you very much.

Senator PRYOR. Thank you, Senator Akaka. Thank you for being here. We will have other Senators join us. We have a quorum call on the floor right now and they are trying to work out some amendments down on the floor, so it is a busy day, but hopefully we will have people coming in and out of the Subcommittee hearing.

What I would like to do now is take a couple of minutes to introduce all five of our panelists and then I thought I would allow you all to make your opening statement, and then we will have questions.

Our first witness will be Alfonso Martinez-Fonts, Assistant Secretary for the Private Sector Office at the Department of Homeland Security. Mr. Martinez-Fonts works to provide America's private sector with a line of communication to the Department.

Our second panelist will be Marko Bourne, Director of Policy and Program Analysis for the Federal Emergency Management Administration. He has had over 20 years of experience in governmental and legislative affairs, marketing, and the emergency services and management fields.

Our next panelist will be Duane Ackerman, member of the BENS Business Response Task Force and former Chairman and CEO of BellSouth Corporation. Mr. Ackerman is the immediate Past Chairman of the National Council on Competitiveness and the National Security Telecommunications Advisory Committee.

Next, the panelist who needs no introduction here, Senator John Breaux, a very respected member of the Senate family. He is a former Senator of Louisiana and Co-Chairman of the BENS Business Response Task Force. He is currently Senior Counsel at Patton Boggs, where he has provided strategic advice on public policy matters since his retirement from the U.S. Senate in 2005.

And last but not least is Dr. Richard Andrews, Senior Advisor for Homeland Security at the National Center for Crisis and Continuity Coordination. Dr. Andrews is also a member of the President's Homeland Security Advisory Council, the World Bank's Disaster Management Operations Group, and former Director of the Office of Homeland Security for the State of California.

Mr. Martinez-Fonts, we will turn it over to you.

TESTIMONY OF ALFONSO MARTINEZ-FONTS, JR.,[1] ASSISTANT SECRETARY, PRIVATE SECTOR OFFICE, U.S. DEPARTMENT OF HOMELAND SECURITY

Mr. MARTINEZ-FONTS. Thank you, Mr. Chairman. Chairman Pryor, Members of the Subcommittee, thank you very much for the opportunity to appear before you today.

My written statement goes into great detail on how the Department and specifically the Private Sector Office, which I head up, communications and collaborates with the private sector. We also illustrate how we work with the component agencies like FEMA to promote the creation and sustainability of public-private partnerships.

In my remarks before you today, I would like to first give you some background on the statutory mandate of the Department of Homeland Security's Private Sector Office. Then I will talk about how we approach partnership building with the private sector. And finally, I would like to conclude my remarks by illustrating how we work with FEMA, CVP, and ICE,

IP, and other component agencies at the Department, encourage and foster public-private partnerships which assist in the integration of the private sector in emergency preparedness, response, and recovery while maintaining the economic health of the economy.

To begin with, let me introduce to you the unique function of Homeland Security's Private Sector Office. As part of the 2002

[1] The prepared statement of Mr. Martinez-Fonts appears in the Appendix on page 59.

Homeland Security Act, specifically Title I, Section 102(f), Congress created the position of Special Assistant to the Secretary for the Private Sector. Comprised of a staff of 14 employees, the Private Sector Office executes outreach, research, and analysis based on its statutory mandates to communicate, engage, and cultivate partnership-building with the private sector. We also act as an advocate for the private sector when we advise the Secretary on the impact of the Department's policies, regulations, processes, and actions.

In order to carry out our mission and to reach approximately 30 million businesses in America, we must have partners. Our principal partners in this task are trade associations and Chambers of Commerce that businesses belong to. Without them, we really simply can't do our job. These associations and Chambers of Commerce include the U.S. Chamber of Commerce, the Business Roundtable, the National Association of Manufacturers, Business Executives for National Security (BENS), National Federation of Independent Businesses, and hundreds of others. We believe partnership-building enhances our Nation's ability to prepare for, respond, and recover from acts of terrorism and natural disasters.

Public-private partnerships cover a range of purposes and members. They come together to exchange information, facilitate dialogue, or focus on a particular set of issues. They can be diverse in composition, ranging from individual businesses to non-governmental organizations.

Partnerships, like organizations, have characteristics which lend to its success. We believe there needs to be a defined mutual goal, a champion on each of the two sides of the partnership, and a business case for action.

As with any collaborative effort, there are challenges which can make a public-private partnership vulnerable. There are three areas that we consider to be potential risks. One is the issue of liability and who bears it. The second is the lack of commitment to the partnership. And the third one is a conflict of interest, which can be real or perceived, that prevents the private sector from fully engaging with the government for fear of losing an economic opportunity.

Homeland Security actively promotes and coordinates public-private partnerships.

It is woven into the very fabric of our mission. We reach out across our Department to our components, who assist them in the outreach efforts to the private sector.

For example, we work with the Office of Infrastructure Protection and their Sector Coordinating Councils where private sector partners represent the 17 critical infrastructures and key resources. We also work with the Office of Intelligence and Analysis to encourage States to include private sector representatives in their Fusion Centers, and we have helped them to develop a model on how to include them.

The Private Sector Office staff is assigned to a portfolio that cover all of the operating components, such as Customs and Border Protection, Immigration and Customs Enforcement, TSA, and Coast Guard within the Department of Homeland Security. The Private Sector Office often acts as a catalyst with Homeland Secu-

rity component agencies to cultivate and foster these public-private partnerships.

We especially work with component agencies to assist in establishment of relationships, integration, and partnership building with the private sector.

What I would like to do today is take FEMA as an example. We have detailed a senior staff person from our office to assist FEMA in their efforts to integrate the private sector into their communications, operations, and logistics. We currently are working to develop a Loaned Executive Program where FEMA can benefit from private sector expertise in logistics and other missions.

We are implementing lessons learned. For example, the Private Sector Office created the National Emergency Resource Registry (NERR), as a result of the 2004 Florida hurricanes. This electronic system was created to manage offers of unsolicited goods and services. However, a year later during Hurricane Katrina, NERR was operational, but was unable to adequately handle all of the offers made to the system. To replace NERR and to address the need for a robust donation management system during a crisis, we assisted FEMA in reaching out to AIDMATRIX, a nonprofit organization who through a grant from FEMA has created a virtual superhighway for all levels of government, private sector, and nonprofits to connect and share unsolicited offers of products, services, and volunteers. Subsequently, the NERR framework has been retooled to create FEMA's Debris Contractor Registry. We are also working with FEMA's National Exercise Program to incorporate private sector in major exercises like TOPOFF 4.

In addition to working with FEMA, we also reach across the Department to find ways where we can encourage the use of standards and best practices just to get things done.

We also work to encourage the adoption of the NFPA 1600 at the local level. For example, we recently held with the U.S. Chamber of Commerce a pilot initiative to create a Regional Business Preparedness Summit in Charlotte, North Carolina. This event brought together local leaders in the emergency management area, public health, and the private sector.

We also collaborate with our Federal partners, for example, with the Office of Infrastructure Protection. We reached out to the Department of Energy to encourage owners and operators of gasoline stations to wire and install generators to operate fuel pumps in case of a power outage.

Public-private partnerships are not disguised charity by the private sector. Good public-private partnership provides common ground towards working towards mutual goals. Public-private partnerships are not a means to shift the public burden away from the government. However, a partnership in its truest state is where both partners contribute their skills and services as a joint effort. This collaboration creates an environment which builds trust, communication, and cooperation. These results only enhance our Nation's ability to better prepare for, respond to, recover from, and mitigate against an act of terrorism or natural disaster.

This concludes my opening remarks. I look forward to answering any questions that you may have.

Senator PRYOR. Thank you. Mr. Bourne.

TESTIMONY OF MARKO BOURNE,[1] DIRECTOR OF POLICY AND PROGRAM ANALYSIS, FEDERAL EMERGENCY MANAGEMENT ADMINISTRATION, U.S. DEPARTMENT OF HOMELAND SECURITY

Mr. BOURNE. Thank you, Mr. Chairman, Members of the Subcommittee, and thank you for the opportunity to appear here today on behalf of FEMA and the Department of Homeland Security. My written statement goes into a lot of detail on many of the new business and management processes that we are putting in place at FEMA in what Administrator Paulison calls the new FEMA. In my remarks to you, though, I would like to focus on some of the key elements of our strengthening relationships with the private sector and our other partners that we are already beginning to see the benefits of.

We are working diligently to build a new FEMA that is stronger and more nimble. With expanded authorities and resources provided to us by this Congress and the Administration, we have implemented a reorganization which I had the privilege to lead, and that we have begun to strengthen our existing structure and fully incorporate the core elements of the former DHS Preparedness Directorate into our organization as part of the new FEMA.

One of the first ways we used our relationships in the private sector can be seen in how we got the ball rolling on many of these organizational reforms. At the end of last year, Administrator Paulison instituted a series of 17 independent assessments. They were agency-wide and they reviewed our existing processes and business practices and included recommendations for reform that were built upon public and private sector best practices. FEMA has already instituted many of the recommendations and we are continuing to do so for the remainder of this year and into the next fiscal year. These assessments have also been an essential resource during our reorganization process.

With our new structure in place, today, FEMA is focused on improving its relationships with the private sector in key areas, such as preparedness partnerships, internal organizational assessments, enhanced supply stream management, logistics, contracting, catastrophic planning, strong community coalition building, and industry fairs and outreach programs.

As the Subcommittee considers private sector preparedness efforts and challenges, at FEMA, we are working closely with the Private Sector Office, the Office of Infrastructure Protection, the Office of Public Affairs, and others to strengthen the outreach to our critical partners in our response to any emergency.

I am happy to note that it has been a two-way street. Many of the businesses that we reach out to and work with are taking active steps to implement recommendations contained in the Ready Business Program, which FEMA had a part in creating, and we are looking at more ways for business to reach out to emergency management at the community, State, and Federal level to participate in planning for disasters that may affect the cities and regions in which they work and serve.

[1] The prepared statement of Mr. Bourne appears in the Appendix on page 72.

FEMA is also engaging the private sector to assist us in our efforts to build an even stronger emergency management system. We are doing so through our Infrastructure Protection Programs, which consists of legacy grants, namely the Port Security Grant Program, Transit Security Grant Program, the Inner City Bus Security Grant Program, and the Trucking Security Program, as well as through our exercises and training venues. The details of many of those programs are contained in my written testimony.

Increasingly, we are leveraging the resources and expertise of our partners in the private sector and nonprofit world, even above and beyond the important role they played in the past. This increased reliance comes about because the new FEMA is developing some innovative ways to move forward to be forward-leaning, quicker to respond appropriately to disasters and emergencies as a partner to our State and local emergency management partners.

One way we are doing this is through a dramatic increase in our pre-scripted mission assignments and our pre-negotiated contracts to provide the necessary resources. Since Hurricanes Katrina and Rita, FEMA has worked aggressively to award hundreds of pre-negotiated competed contracts and these are in place and ready for the 2007 hurricane season. This is allowing us to be prepared ahead of a disaster so we are not negotiating contracts in the heat of battle. Contract agreements are in place covering all aspects of FEMA's disaster management, to include logistics, mitigation, individual assistance, recovery programs, management, and integration center support.

Perhaps the most visible example of how the private sector has influenced FEMA's reorganization is through the creation of our Logistics Management Directorate. Our goal is to have our logistics management look at business practices that are in place and understood by the community across the country rather than reinventing the wheel ourselves. We are moving towards an increased ability not only to track the commodities that we do keep and maintain, but to begin to shorten our supply chains and look to third-party logistics to handle the majority of the resource needs in a just-in-time delivery. We have looked at AIDMATRIX and adopted it to support our supply of donated goods and services.

Through our Citizen Corps Program, we are bringing community and government leaders together in all-hazards emergency preparedness planning. There are 2,200 Citizen Corps Councils with a presence in every State and territory. Councils are encouraged to include business representation and to work with business to integrate those resources with community preparedness and response plans.

As we look to FEMA's preparedness efforts, we believe the private sector should continue to build upon their preparedness efforts in several key areas. First of all, to continue their development of strong business continuity plans for all of their locations and critical data centers. Develop employee support plans for their employees' office locations that are damaged or if they have employees that have lost their homes. Part of the issue in quick recovery from a disaster, or quicker recovery, is the element of getting people back to work as soon as possible in the affected areas.

We encourage them to engage in prudent risk management practices and have strong health and safety programs, working closely with their local emergency managers and first responders and elected officials to be involved in disaster planning that begins at the local level and builds to the State. To build protocols to assist with recovery efforts before a disaster strikes.

Through business associations, we are continuing to work with State emergency management and FEMA to support preparedness planning, disaster response, and donation management. The private sector has also engaged FEMA and State emergency management and offered to provide liaisons to State Emergency Operations Centers, Joint Field Offices, and we are working with the Chamber of Commerce, BENS, and the Business Roundtable and others in developing a private sector association liaison, which we hope to be able to put into the National Response Coordination Center here in Washington.

FEMA is also integrating the private sector in a myriad of initiatives across the agency. For example, we are working closely with Homeland Security's Private Sector Office to utilize their concept of relationship and partnership building. We have welcomed the Homeland Security Private Sector Office Staff as part of our senior advisors. And a number of initiatives that we are undertaking will involve communications outreach and operations in mission critical areas, like logistics.

Just a highlight of our new approach to the private sector include many things which also involves a meeting next week that we had scheduled prior with BENS, BRT, and the Chamber together to discuss new initiatives that we can take to move this agenda forward. We want to take a proactive approach to leading the way for the private sector to be incorporated in our emergency operations and especially working for ways to find access that we can bring in association representatives into the Joint Field Office and Regional Response Coordination Centers.

We are incorporating private sector expertise by creating a new FEMA Loaned Business Executive Program. We hope to, in the next few days, close an agreement with a business foundation which we will name after we have the agreement finally signed which would bring a seasoned expert from the private sector into FEMA operations to serve as an advisor and collaborator on mission critical programs. This is a start of a program we hope to expand in the future after we have had an opportunity to see how it works.

Private sector participation in our Regional Emergency Communication Coordination Groups, which we will be standing up over the next several months, is also critical.

We are developing a Memorandum of Understanding with the Stadium Owners and Operators Association for sheltering.

We have funded a pilot program in Denver with InfraGard and BENS to support a resource registry that can be utilized at the local level to improve the private-public partnership.

We encourage mutual aid programs for businesses. We can provide mutual aid training through our online systems at the Emergency Management Institute, and we can provide a pilot website to serve as a repository to post information about all of the above ac-

tivities, training opportunities, and business continuity programming.

Our regional offices have been reaching out to the business community. For example, Verizon wire and wireless has met with our Region 1 office in the last 2 weeks with regard to hurricane planning, and our Region 5 office is working with ChicagoFIRST on preparedness planning for financial institutions.

We are also going to be establishing a credentialing working group within the NIMS Integration Center to pinpoint some of the issues on credentialing and develop some viable options to address the credentialing concerns.

There will certainly be a continuing role for the private sector in the future at FEMA. FEMA needs to ensure that we are adapting to new conditions and the ever-changing needs. It is important that as we build these relationships, we continue that effort so that it is understood by all parties that you can't just show up on game day and expect to play without being part of the practices. Our job is to make those practices available, open, and valuable for both us and the private sector. FEMA realizes that a successful, robust, coordinated response is needed and that the private sector, both horizontally and vertically across the full spectrum of emergency management, is a partner.

Thank you for the opportunity to be here today and I look forward to answering any questions you might have.

Senator PRYOR. Thank you. Mr. Ackerman.

TESTIMONY OF F. DUANE ACKERMAN,[1] FORMER CHAIRMAN AND CEO, BELLSOUTH CORPORATION, BUSINESS RESPONSE TASK FORCE, AND MEMBER OF BUSINESS EXECUTIVES FOR NATIONAL SECURITY (BENS)

Mr. ACKERMAN. Mr. Chairman, Members of the Subcommittee, I want to thank you for the opportunity to be here today. When I think about the work that has been done on the task force, I did have the privilege of serving on this task force and developing the report which you have had. And while we don't have time to go through every single detail, I would like to just stipulate, or I would like to ask that my written testimony be submitted along with the complete report for the record. Then I would like to focus my time on this issue of the public-private partnership and some of the work that we did on the task force to look at the private sector and examine its role in disasters.

First of all, we found that on a local scale, disasters do happen right regularly, and business routinely plans and interacts with first responders and collaborates on those disasters at the local level. We have also found that after securing their own businesses, they invariably turn towards the rest of the community because without community continuity and without business continuity, surely there is no recovery in that community and there is no business done. So it is clear that business does have an interest that goes beyond their own operations.

We have dealt with many hurricanes, but indeed, Hurricane Katrina was different, as has been mentioned and talked about

[1] The prepared statement of Mr. Ackerman appears in the Appendix on page 85.

over the years. It was a terrible tragedy, but I think there are some very key issues that evolved from Hurricane Katrina that are instructive to us as we look forward to what may lie before us.

It had many characteristics that a large natural and/or manmade disaster will have as we go forward. Major damage to critical infrastructure. Contamination—in the case of Hurricane Katrina, it was water. In the future, it could be other things, such as nuclear, biological, or chemicals. Overwhelmed law enforcement and the breakdown of civil order was present and Federal help was required; but there was no real plan for integrating all of the concerned entities for a response. The Federal Government has a plan. Certainly the State has a plan. Local has a plan. Business has a plan. But there is no plan for all of these entities in terms of how they are going to operate and function together at the time of crisis.

I think all of the above conditions would be present in a disaster that impacted a significant portion of any major metro area, whether it is a natural disaster or manmade.

Our Subcommittee looked at known problems from Hurricane Katrina. We looked at recommendations that came from over 100 interviews that were made with the private sector. We drew on the knowledge of both the public and private sector in order to pull our study together. We conducted face-to-face meetings in Washington, DC. Various meetings were held and we brought all that back together in order to produce the report, "Getting Down to Business."

The overall conclusion was the private sector must be included in the planning, practice drills, and execution of a disaster response scenario. I would certainly like to emphasize practice in this regard, because I think it is one thing to have a plan, but until you have had the Federal Government, State government, and local authorities and the private sector at the table, certainly, I don't believe we have accomplished the task, and there are a lot of reasons for this.

First of all, the private sector owns much of the infrastructure. The private sector has experience, skills, information, and capabilities that are critical to a successful response to a major disaster. And we believe that once local and State capability is overwhelmed, the Federal Government always will be called on and will be expected to help, and when they come to help, that interface with the other entities and how they will make decisions and how they will partner becomes very important.

We use this term public-private relationship frequently, but when you think about what it means in this case, it absolutely means that most of the States have an Emergency Operations Center and what we are suggesting with the BENS report is that there be a companion Business Operations Center either at the State or the regional level at the same time, and that needs to be able to expand to incorporate the Joint Field Office when it comes with the Federal agencies so that all parties can collaborate along with the private sector on the immediate challenges, threats, and the solutions that must be implemented.

So we believe that the National Response Plan needs to include the private sector. It needs to support joint planning, joint practice drills, and when an event occurs, joint execution. Joint in this case means local, State, Federal, and the private sector.

Practice, again, is extremely important, because by conducting joint drills, we constantly turn up new issues, new problems that must be overcome and must be overcome together.

It is my hope and the sincere recommendation of the BENS Task Force that you will acknowledge, encourage, and support the building and exercising of enduring public-private collaborative partnerships that integrate the private sector into the National Response Plan and the National Response Infrastructure. In turn, the private sector must have a reliable government partner, and the emphasis there is on the word "partner" because viable regional and Federal actors in all phases of the operations must relate to each other in balanced proportions in order to come out with a successful ending.

If this structural reform is indeed adopted, it will greatly facilitate all of the other recommendations in the report of the BENS Business Response Task Force. Thank you.

Senator PRYOR. Thank you. Senator Breaux.

TESTIMONY OF HON. JOHN BREAUX,[1] FORMER U.S. SENATOR FROM THE STATE OF LOUISIANA, CO-CHAIR, BUSINESS RESPONSE TASK FORCE, BUSINESS EXECUTIVES FOR NATIONAL SECURITY (BENS)

Mr. BREAUX. Thank you very much, Chairman Pryor and Senator Akaka. Thank you for making time in your very busy schedules today for us to make this presentation, and also Senator Sununu, thank you for coming back. The place looks a lot better since the last time I was here. The chairs are much more comfortable, I want to tell everybody, but we will not overstay our welcome and make it as brief as we can.

I would like to ask unanimous consent that my full statement be made part of the record. I will just try and summarize, if that is all right.

Senator PRYOR. Sure.

Mr. BREAUX. I accepted and volunteered after Duane Ackerman, our chairman, called me and asked me to volunteer, and you can't tell Duane Ackerman no, to serve as co-chair with Newt Gingrich of this effort, which I think has been very productive and hopefully very helpful to the Members of Congress who are looking for ways to try and find out what we can learn from natural disasters that occur.

A natural disaster, as bad as it is, is terrible, but if we don't learn anything from it, it is a double disaster, and I think that now that we have had time to reflect on Hurricane Katrina as one of the largest natural disasters in the history of the United States, there are things that we can recommend that we know that can be done to make sure that the next time these things happen, that we can be in a better position to respond effectively and quickly and be helpful to the citizens of this country.

We can work in Congress to prevent disasters like what happened on September 11 by having stronger national security, and by having a strong military. We can help prevent September 11s. But we can't, no matter what we do, ever prevent another hurri-

[1] The prepared statement of Mr. Breaux appears in the Appendix on page 91.

cane. We can't prevent another flood. We can't prevent another earthquake. But we can, through Congress, try to make sure that we are better prepared to respond to these type of natural disasters when they occur, and I know your Subcommittee, Mr. Chairman and Senator Sununu, are working hard to come up with recommendations, and hopefully what we are presenting to you can be helpful in that regard.

One of the things that I think that we would like to recommend is that this involvement of the private sector needs to be better institutionalized. Director Marko Bourne and Secretary Al Martinez-Fonts, I am delighted to hear what you all have done to integrate the private sector. That is real progress that they have talked about here this morning.

But I think that, in addition to that, the process has to be more formalized. It has to be institutionalized. It has to be in writing. It has to be out there so that the private sector can know exactly what the rules and what the regulations are when a natural disaster occurs, and I think that this Subcommittee could be particularly helpful in focusing on institutionalizing an effective and sustainable role for the private sector, and that is incredibly important.

We made recommendations in three principal, substantive areas. Mr. Ackerman talked about the public-private collaboration, incredibly important. Government can't do this by ourselves. The private sector must be involved. After Hurricane Katrina, people talked about, well, what we ought to do is have government facilities, distribution centers by the government set up around the country. We don't need government distribution centers. We have got private sector distribution centers. Senator Pryor, Wal-Marts are in every State in the Union. Whether it is a Wal-Mart or a Home Depot or a Lowe's or any of the large distribution centers, they are already there. The challenge for government is to incorporate the government's work with the private sector to make full utilization of the supplies that are already around the country located in key areas that are very accessible and already there.

We also are making recommendations on surge capacity for the private sector goods and services.

How do you gear up quickly for a natural disaster? I think the two government witnesses have made good comments in that.

I would like to focus quickly on the legal and regulatory environment. I think that is important. Businesses require some type of a predictable legal regime before they get involved in helping. We had people that came down from Arkansas and people that came down from all over the country. They didn't know what the rules were in Louisiana. They didn't know what the laws were in Mississippi or along the coast. They didn't know what they could do and how they could do it. There has to be some type of a system in place for these private sector groups, and when they want to come down and help, they know what the rules are going to be.

We also have to, I think, reform to a large extent the legal allocation of risk to private companies when they are willing to help. We heard from a lot of companies, Mr. Ackerman, that said, look, we wanted to be involved, but we didn't know what our liability was. So if we come down there and we do something not quite right,

what is our legal responsibility? As a result, some private sector companies said, well, we are not going to do it because we don't know what the risks are. It is not a reasonable risk for us to accept on behalf of our stockholders.

I will give you a real example of that. When New Orleans was under water with about seven, eight, to ten feet of water throughout the city, contracts were issued by the government to do what we call de-watering of the city, and what they were ordered to do was to take the water in the city and pump it out into Lake Pontchartrain. Nobody got a permit. There wasn't an EPA permit or a Corps of Engineers permit to do that. And the companies were saying, well, what if we do it, we don't have a permit, and somebody is going to sue us after for polluting the lake? Well, there is a question of priorities. The city was under ten feet of water and people were drowning and you are going to say, well, we can't do it until we get a permit from the government and go through the permitting process? That can't be done.

But companies, when they approach these emergency situations, have to have a very clear understanding of what the legal requirements are when they become involved, as a volunteer in many cases or as a private contractor in others, but they have to know what their legal exposure is and so they will have a clear ability to make the right decision. I think that is something that we could do very well with amendments to some of the laws that are in place.

We would like to, in other words, enact a national disaster law. We have the Stafford Act, a great program, and all of you folks and the staff are very familiar with it. But we would like to suggest that the Stafford Act also has to include the private sector. It can't just be local governments and State governments. The private sector ought to be incorporated and brought into the Stafford Act so they will know under that Act of Congress exactly what their roles can be, what their exposure can be, and how they can be greater involved.

I think it would be just absolutely terrific if this Subcommittee could focus on some hearings on the Stafford Act. You can't do it really quickly. You have to do it carefully. This is a law that has been around for a long time. I served with Senator Stafford when he was here and wrote this and I think that it served us greatly, but it ought to be changed in order to bring in the private sector and make it a part of the Stafford Act, as well. It covers State and local. It needs to cover private sector, as well.

Finally, let me just suggest that a lot of the things that we are talking about to get the locals and the States involved, I mean, you could require that when you get a Federal grant under FEMA that a State have in place, without any cost to Congress right now, a mechanism to incorporate the private sector. Every State ought to have a clearly defined plan that when a natural disaster occurs, and we know it will, that they have a plan in place to bring in the private sector to help them solve the problem. That can be a requirement for getting any kind of a Federal grant. If they don't have the plan in place, they are not eligible for Federal grants, and you wouldn't be surprised how fast States would move in that direction if they knew their Federal assistance was dependent on

having a well-established, clearly thought out local plan on the State and local level to involve the private sector.

One thing that we found, Mr. Chairman and Members, in all of our meetings that we had is that you have in place a private sector community that is ready, willing, and very able to help our Federal Government address these natural disasters. We need to clean up some of the laws and some of the provisions in order to make it possible, but I think that this Subcommittee certainly has the great leadership and great capacity to make that happen.

Senator PRYOR. Thank you. Dr. Andrews.

TESTIMONY OF RICHARD ANDREWS, PH.D.,[1] SENIOR ADVISOR FOR HOMELAND SECURITY, NATIONAL CENTER FOR CRISIS AND CONTINUITY COORDINATION

Mr. ANDREWS. Thank you, Mr. Chairman, Members of the Subcommittee, and thank you for the opportunity to testify today. I served as a member of the BENS Task Force that developed the report that has been referenced in the previous testimony. I am also Chair of the Private Sector Committee of the National Emergency Management Association (NEMA), which is the association of all the State Emergency Services Directors, and served as former Director of the California Governor's Office of Emergency Services and Homeland Security Advisor to Governor Schwarzenegger.

My testimony today focuses on my work as Chair of a public-private sector task force that was formed following the release of the BENS report to start working on implementing what I think is one of the key recommendations from the BENS report which has been referenced by both Mr. Ackerman and Senator Breaux, and that is to try to develop a systematic process for incorporating private sector resources into the response to a major disaster.

Hurricanes Katrina and Rita created the largest demand for emergency resources in our history, and each of the major after-action reports cited the Emergency Management Assistance Compact (EMAC), which is the compact formally adopted by all the State legislatures for which NEMA serves as the executive agent, they all cited EMAC for its success in mobilizing tens of thousands of National Guard, search and rescue, medical and emergency management personnel.

The BENS report identified also an obvious shortfall of the 2005 hurricane response, and again, it has been referenced in previous testimony, namely the absence of a systematic process to utilize private sector resources. A number of different efforts, especially the creation, as Mr. Martinez-Fonts mentioned, especially the creation of the National Resource Registry by DHS's Office of the Private Sector Coordinator laudably attempted to fill this gap, and while there were some successes, there was a great deal of frustration both within the public and the private sectors. Each recognized the need for greater collaboration, but the absence of a commonly understood process to match needs with available resources, whether those were donated resources or contracted resources, proved to be a major obstacle.

[1] The prepared statement of Mr. Andrews appears in the Appendix on page 97.

Among the recommendations in the BENS report was the idea of building a Business Emergency Management Assistance Compact (BEMAC), modeled essentially on the EMAC system that proved so successful during the 2005 hurricane season. By expanding EMAC, it might be possible to weave together a fabric of State-based Business Operations Centers where private sector representatives trained in the State's operations system would work alongside emergency management leaders to coordinate government and private sector resources.

Earlier this year, the NEMA Private Sector Committee began to explore whether this concept could be implemented. BENS supported this effort by assigning staff resources, and my own company, NC4, endorsed my chairing this effort. Representatives from eight national corporations, many of which have been mentioned in earlier testimony, along with the EMAC leadership—this is the Directors of State Emergency Management who oversee the EMAC process—served as members of the task force.

One of the task force's basic premises was to build on existing State and local initiatives and to focus, like EMAC, on the interstate deployment of resources. In order to establish an understanding of existing State and local initiatives, NEMA conducted a survey of all the States. The survey identified a number of very promising initiatives at the State level to work with the public and private sectors, and a few examples stand out and are worthy of mention.

The Florida Office of Emergency Management has formally established Emergency Support Function 18, Business, Industry, and Economic Stabilization. ESF 18 works with the Florida Retail Association to address strategic supply chain issues, projected impacts on businesses, and the timely restoration of commercial services.

Texas, in the aftermath of Hurricane Rita, has developed an extensive Private Sector Operations group consisting of 28 companies to support immediate mass care, special needs, power, aviation, and fuel challenges. This group will work alongside State emergency management to identify shortfalls in public sector capacity that could be most effectively met by private sector resources.

Utah is organizing sector-specific coordinating councils and is working with local Chambers of Commerce and trade associations to enhance communications, resource management, and emergency operations assignments.

The New York City Office of Emergency Management has fully integrated the private sector into their processes at their new Emergency Operations Centers. There are also important initiatives underway in the State of New Jersey, the State of Georgia to create a Business Operations Center that Mr. Ackerman referenced, in the State of Massachusetts, and also a beginning initiative in the State of California.

Nevertheless, a number of significant challenges remain, especially related to using private sector resources in interstate responses. Only four States have statutory provisions that enable private sector resources to be used as agents of the State in out-of-State deployments. Those are Delaware, Michigan, Maine, and North Carolina. Other States have specific statutory or procurement regulations that appear to preclude such arrangements.

A fundamental premise of EMAC is that personnel and equipment deployed out-of-State must act as agents of the providing State. Other States have stringent restrictions on what pre-event contracts and arrangements can be negotiated with the private sector, and in many cases, apparent prohibitions against applying those contracts to a response into another State.

The BEMAC Task Force has identified several next steps that we believe will help create a more clearly understood process by which the private sector can be mobilized across State boundaries, and I would emphasize that these are really the initial steps, and much like the starting of EMAC in the aftermath of Hurricane Andrew in 1992, we believe it is important to take small but real steps as we move towards a more robust and systematic national process.

BENS has agreed that in cooperation with the U.S. Chamber of Commerce and the Business Roundtable, they will work with the Department of Homeland Security to identify the point of contact for each of the critical sectors. NEMA, in turn, will brief the critical sector points of contacts on the EMAC process and will promote the use in each State of the points of contact to coordinate requests for private sector resources.

NEMA will also develop a document detailing best practice procedures by State and local governments for working with the private sector and will distribute this report to State Emergency Services Directors as well as to the various sector coordinators.

NEMA will work with our task force to define in detail mission critical packages of resources projected to be needed during an emergency response, and again, this is to try to create the anticipated need in advance so that we are not trying to put these packages together on the fly.

And NEMA and the BEMAC Task Force will work with FEMA to address issues related to reimbursements for private sector resources and compensation for services used through an EMAC-like process.

These steps, we believe, will advance the use of private sector resources by State and local entities and help clarify for the private sector a process to be used in requesting resources. States will remain the primary coordinating point for inclusion of the private sector under this paradigm.

Clearly, FEMA needs to be an active partner in this process. The scale and variety of risks facing this Nation from natural and manmade emergencies necessitate that we make full use of our public and private sector resources. Only through such cooperation partnerships can we accelerate individual and community economic restoration and recovery.

Again, thank you very much for having me here today. I look forward to your questions.

Senator PRYOR. Thank you.

We are going to go out of order today and we are going to let Senator Akaka go first. Senator Akaka.

Senator AKAKA. Thank you very much, Mr. Chairman.

Mr. Ackerman, I believe strongly that we need an all-hazards approach to preventing, responding to, and recovering from disasters. I am pleased with your written testimony and pleased with the BENS report emphasizing planning for both natural and manmade

disasters. In your experience, has the Federal Government been as aware as the private sector of the need for all-hazards disaster planning, and if not, what should the government be doing?

Mr. ACKERMAN. Thank you. When I think about the many years I have spent in disaster recovery because of the telecom industry, many of these disasters have been local or have been able to be handled at the State level, so there has been a great deal more practice at a State, private sector, local response. In the area which I am very accustomed to, which is the Southeast Coast, we have had a lot of practice. We have had, probably in my 40 years, over 50 hurricanes that have come on that coast and it seems to work very well because of the relationships that have been built over time.

When a disaster overwhelms local capability, which we could expect in either natural or manmade at Hurricane Katrina-scale or larger, that is the point in which the Federal Government then comes to the location. And so it is as important to drill and practice with the private sector and plan as it is with the Federal Government because often, it is new relationships, it is different operating procedures, and it is day-to-day decisions that have to be worked out . . . how the Federal Government works as a full partner with the State, with the local, and with the private sector.

FEMA is a big part of this, but it is not just FEMA. North Command is a part of this. DHS obviously is a part of this. So as you create the Business Operating Center and integrate that with the State and local, there also needs to be the ability to bring in and interface the Federal Government, both at North Command, FEMA, as well as DHS, whatever agencies are there. And that collaborative whole hand needs to be able to drill scenarios and practice scenarios to determine how one would work out issues as opposed to trying to work that out when the actual disaster occurs.

Mr. Bourne talked about credentialing. Well, that was born out in the case of Hurricane Katrina when North Command came to town and set up a perimeter. We needed to cross that perimeter in order to work on facilities, but a new perimeter was there and then the question was, what credentials proved that you were a valid communications worker and what credentials would the Federal Government accept as opposed to what credentials the State and what credentials you would find at the local level?

So there are numerous issues that will need to be worked out with all parties at the table before the next event. So I think that it is a disaster of scale, one where local capability is overwhelmed, where everyone has to come to the table and to try to work through how we accomplish our task, deliver our missions, and assist each other to enable the recovery of that local area as opposed to just having the Federal Government come in with a plan.

As I stated in my testimony, I think everybody has a plan. The lacking plan is how we all work together when the Federal Government comes to town, short of martial law, which no one really wants to declare. So I think this issue is one of full integration, planning, practice, as well as execution, including the private sector, local, State, and the Federal agencies that will be involved in disaster response.

Senator AKAKA. We really appreciate the BENS report, "Getting Down to Business: An Action Plan for the Public-Private Sector Disaster Response Coordination," and your experience really makes a difference in how we move that.

Senator Breaux, you testified that DHS grant programs currently are geared to funding one-off exercises rather than long-term collaborations. Project Impact, which was established in 1997 but eliminated in 2001, focused on long-term continuity projects to identify risks and vulnerabilities and develop programs to lessen those risks. These projects involved both the public and private sectors in disaster planning. Although FEMA now provides pre-disaster mitigation grants, as you stated, these are focused competitive grants not directed toward ongoing collaboration.

Senator, do you believe that Congress should restore funding for programs such as Project Impact that focus more on long-term collaborative planning?

Mr. BREAUX. I think that anything that gets the Federal Government four-square behind additional cooperation between local governments, State governments, with the private sector would be very helpful. I have thought of suggesting that grants to States under FEMA be conditioned on the States having in place a plan for involvement of the local business community so that the business community will know what to do, and that wouldn't cost anybody any additional money. The grants are already going to the States. I think the Federal Government could insist that the State have in place a workable private sector continuity program that would immediately kick in in the event of a natural disaster. I think that would be one way to accomplish this.

I mean, this is something this Subcommittee and Congress could insist on, that Federal grants would be conditioned on the State and local government having a plan to involve the local private sector. It wouldn't cost you any additional Federal money, but I guarantee you the State and local government would follow that recommendation from Congress very quickly.

Senator AKAKA. Thank you. My time is expired, Mr. Chairman.

Senator PRYOR. Senator Sununu, thank you for being here today and being a great Co-Chair. I look forward to working with you on this.

OPENIN STATEMENT OF SENATOR SUNUNU

Senator SUNUNU. Thank you.

Mr. Ackerman and Senator Breaux, a question for both of you relating to the BENS report. One of the things that was recommended were changes to the Stafford Act. I am curious to know, one, what specific changes need to be made and is changing the Stafford Act intended to address a specific recommendation or just a few recommendations or are all of the recommendations that you call for sort of encompassed by the Stafford Act? And are there potential unintended consequences to changing the Act, because you also emphasized the need to be deliberative about this. Is there any particular unintended consequence about which you are most concerned? Mr. Ackerman.

Mr. ACKERMAN. Yes, Senator. I can give you an example of the kind of thing that sort of generated an early focus on the Stafford

Act and it had to do with security. Security is offered to certain government entities, to the Red Cross, and to others. It is a little bit more questionable as to how that relates to the private sector.

Again, if you have a disaster that takes out some piece of a large metropolitan area, there is a likelihood that you will have some civil disorder go along with that if it overwhelms local capability.

In the case of Hurricane Katrina, we needed to move into the city to work in some areas that had a problem and there was a question about does the Stafford Act include or cover providing the private sector, especially emergency responders, not first responders, but power company, telephone company, computer company, does it provide us security going into an area where citizens are hostile or armed or just bands of people who are horribly upset? And so that caused some delay, caused some consternation, and indeed, there was a very real and a very significant issue. So that is the example of the kind of thing that needs to be addressed in the Stafford Act.

I cannot assure you that there would not be unintended consequences, but it definitely needs to be examined because I think from a response point of view, it is clear that there are some issues that hamper response and that appear not to totally cover the issues that could crop up in a serious large disaster.

Senator SUNUNU. Senator Breaux.

Mr. BREAUX. Yes. I can only add a little bit. Mr. Ackerman hit it right on the head. But, there were some classic examples of trucks being denied access to disaster sites because they weren't a government truck. You are bringing ice down there. Well, you can't cross the line because you are a private sector delivery system. You are not approved to go into that area. And a lot of the local officials and State officials don't understand what is to be allowed and what is not to be allowed.

You all last year amended the Stafford Act to at least prevent under the SAFE Port Act, prevent any Federal agency from denying essential services from the private sector. That is a big improvement, that they can't deny essential services coming from the private sector.

But I think the main thing we are advocating is just bring the private sector into the process. Make sure the States and local governments have a mechanism that the private community is involved in helping to solve the problem. And then that clears up—if they are at the table from the very beginning, helping to devise the plan as part of the team, then these type of problems can go away.

Senator SUNUNU. Mr. Bourne, I think, as of April 1, there was a reorganization at DHS that created the National Preparedness Directorate within FEMA. How specifically is that directorate being used or going to be used to enhance outreach and coordination with the private sector?

Mr. BOURNE. The National Preparedness Directorate is specifically designed as both not only internal preparedness efforts at FEMA and our Federal partners, but really heavily focused on assisting preparedness at State and local levels and private sector. Doing that through—certainly they manage the grant programs that are available, but at the same time—the Citizen Corps Pro-

gram and the Community Preparedness Division within National Preparedness, their job is to reach out to State and local governments, find ways to build collaborative partnerships between the private sector, State, and local governments.

Our other role is to provide a planning framework. Part of the problem is that we all do planning. We do planning in our own circles. We do planning within our own expertise. What we don't have across the Nation is truly a planning community that involves all the folks that need to be involved. That is an evolving and growing thing.

Part of what we are doing as we rewrite the National Response Plan is taking a look at preparedness and planning as an integral part of understanding how a planning community needs to be developed. There needs to be some basic framework so that we are planning to similar objectives, similar principles. We can't all plan exactly alike. We have different capabilities and different needs. But we need to be planning jointly and collaboratively at all levels.

It is very critical, and the National Preparedness Directorate is focused on this, that the planning effort and the relationships that are first and primary are the ones between local business, the private sector, NGOs, and the State and local governments. That is where 90 percent of all disasters happen. It is also, however, critical that FEMA have a good understanding, working through the business associations and other private sector experts, in how we can involve them in our planning, training, and exercise activity. National Preparedness is directly responsible for that effort.

Senator SUNUNU. Mr. Andrews, in your work for the National Emergency Management Association, you obviously come in pretty close contact with people at the State level and some of the State Directors. What do you see the States being most concerned about, and is it your opinion that the States are looking for more Federal mandates for integrating the private sector into their preparedness plans, or are they hopeful that we can do this with a little bit more flexibility and with an approach that recognizes that there are going to be some unique individual needs among the States?

Mr. ANDREWS. In the survey that we did of all the States, and asked them a number of questions about their working relationships, where they were in the process of working with the private sector, 44 of the States indicated that they had some degree of working relationship with the private sector, and again, it ranged from very formal processes, like in the State of Florida, to those States that are essentially just beginning the effort. And I think this really represents a real sea change. I think 5 years ago, the numbers would have been dramatically different.

I don't think that the States are looking for mandates in this area at all. I think that they recognize, for the most part, that there is an advantage to them, and Hurricane Katrina clearly brought home the fact that we can have a disaster that initially appears to be a regional disaster that, in fact, involves all of the States.

And so there has been a lot of work to enhance the EMAC system, and again, EMAC is kind of a cornerstone of the Nation's emergency management capability. All of the National Guard troops that were mobilized to the Gulf Coast, over 60,000 of them,

were done under the authority of EMAC and the enactments of all 50 State legislatures of the EMAC proposal.

I think the States would welcome some additional encouragement from DHS and FEMA to move ahead with this, but I don't think that specific mandates to the States to try to accomplish this are really necessary.

Senator SUNUNU. I appreciate that very much. Thank you, Mr. Chairman.

Senator PRYOR. Thank you.

Let me ask you, Mr. Ackerman, if I can, about some of the things that your company did during the Hurricane Katrina disaster. As I understand it, you opened your Operations Center to many of the major wire line, wireless, and cable providers in the impacted area. I don't know if that was exactly unprecedented, but it sounds like it may have been. I am curious about why you did that and how that worked out and why you felt like that was important.

Mr. ACKERMAN. Thank you.

The primary cause for taking that action was the seriousness of the outage. We knew that with the flood, we were going to have serious outages, landline outages inside the Bowl, or inside the city itself because of the flood. We knew that the wireless carriers were going to have serious problems because many of their links from one location to another were in facilities that were also in the Bowl. And we knew the interexchange carriers were going to have problems.

So we knew that getting signal or communications capability back into the city was of the most—was just of the highest importance, and therefore, we decided the best thing to do, since we were managing and responding to the need to fix local facilities, was to get the carriers into the Operations Center to help us prioritize what was indeed the most important. So we worked hand-in-hand with the wireless carriers. We had representatives from each one of the wireless carriers. We did the same thing by phone with the interexchange carriers. They were a little bit more concerned about being together. But it enabled us to prioritize and get back those facilities that were most important to restoring the most communications back to the local community.

And so seriousness drove it, and we felt the best way was to put everything on the table, get everybody in the room. Again, it is this collaborative effort at the point in time when you do have a disaster of this magnitude that enables success. The more knowledge you have together, the more ability you have to prioritize and make on-the-spot decisions about what goes next. I think that is just incredibly important to restoring service.

Senator PRYOR. And how did that work out? Were you pleased with the way it went?

Mr. ACKERMAN. I think it optimized the process. The damage was significant enough that I think it took us a long time to get facilities back where we would like to have had them. But it did enable us to optimize the process and I think it did enable us to get those most important things back first.

Senator PRYOR. Before Hurricane Katrina occurred, was that part of your plan or did you make that decision on the spot, recognizing the seriousness of the situation?

Mr. ACKERMAN. It was not part of our plan. We made that decision on the spot.

Senator PRYOR. And did the government help you at all on that, or was that private sector initiative?

Mr. ACKERMAN. That was private sector.

Senator PRYOR. Let me ask about private sector logistics and planning. You mentioned the word "practice," and you emphasized that and how important it is to practice, but let me also ask about logistics, delivering goods and services, planning. Your group recommends that the private sector be much more involved with the government in planning. I think that is a great concept and it is very logical to me and it seems like it is something that should be done, but how do we do that and not create a conflict of interest or an advantage for companies who are participating in that planning and that logistical effort?

Mr. ACKERMAN. I don't have a pat answer for that question. It is a good question. What I do know is that we have got to find some way to deal with it because there is such a significant need to be able to run these drills or practice ahead of time. Invariably when we run a practice run on a disaster response scenario, we find something that we had not thought of before and we are able to clear that problem out before we get into the actual event.

So I put an extremely high importance on finding a way to do that. I believe that there are always issues about whether or not that advantages one company versus the other, but at the same time, when the ox does get in the ditch and our citizens are in the situation that they are in, finding a way to be as expeditious as possible is a big help.

It was mentioned earlier today that there is a great deal of work going on on pre-approving vendors and putting contracts into place. I think it was mentioned by Mr. Andrews, also. I think that is an important issue. I think that everyone cringes when the word "price" comes up, but at the end of the day, we need to deal with that ahead of time, not during the middle of the disaster. Again, it is something that begins to slow the progress down.

So it is difficult and it is tough slugging, but I think it needs to be done, and again done in practice drills before we get into the disaster and not after.

Mr. BREAUX. Can I add just a real quick thought to what Mr. Ackerman said?

Senator PRYOR. Sure.

Mr. BREAUX. The ox in the ditch is a good analogy because when a city is underwater, you have to respond immediately, when people are drowning or a fire is going on or right after a hurricane. And there is a difference between getting people in immediately to help in an immediate situation as opposed to the long-term construction and rebuilding. Those things need to be bidded out in competitive bidding. But you have to have a system in place before the disaster to get people in in the immediate aftermath of a disaster and for the first week or so, get the work done that has to be done. Then you can look at the long-term work that needs to be done that has to be competitively bid out and have everybody at the table. But you can't do that when you are waiting to dewater

a city that is underwater. Those people have to be ready to go as soon as the hurricane passes through.

Senator PRYOR. Mr. Bourne, you also were kind of nodding your head during the question and answer there. Did you have a comment on the process? I think I mentioned conflict of interest or advantage—

Mr. BOURNE. It is problematic, and it is problematic for all levels of government. The General Counsel's Office loves to accuse me of playing lawyer without a license. They are rightly concerned that there are regulations and laws that limit how much we can do.

FEMA has taken a very proactive approach to some of this. We have looked at the preplanned contracts that we have done, that we have competed ahead of time to deal with those issues that we anticipate in the first 72 hours and the immediate days following rather than that longer term. There are longer-term recovery contracts that we already do. Readiness costs money, and a lot of times folks blanch at the idea of spending money in the event of something that may not happen. But it is like that insurance policy we all end up buying anyway for our home, which we hope we never have to use.

So FEMA has put in place a lot of these readiness contracts so that we have access to the resources we need to support State and local. But it is also more important, and many State and local governments have begun to do this, that they begin to look at advance contracting and planning, as well, whether it be for debris removal, whether it be for evacuation purposes, for transportation and other items that they may need.

They may never use them. We hope they don't. But the simple fact of the matter is that that work in advance saves a tremendous amount of time and headache in the end. Also, under the current level and regulatory restrictions that all levels of government are under, it is the most efficient way to move resources quickly without getting into an area that we don't want to go back to, and that is no-bid contracts or contracting over a barrel during a disaster.

Senator PRYOR. One last question before I turn it back over to Senator Akaka. My question is for you, Mr. Bourne, and that is what about small business's role? I mean, it is one thing to have these large Fortune 500 companies. They are all great and they can do a lot of things logistically, etc., but what about small business? How do you include small business in the planning phase?

Mr. BOURNE. We have done this in several ways. Certainly, we encourage State and local governments when they look at their planning to bring small businesses in. Most communities, the vast majority of the workforce works for small business. And those kind of critical jobs and critical businesses need to be brought back up to speed in part of the planning process. That has to be done through planning. Also, they are contracting at the State and local level, whether it is pre-contracting or post-contracting. It is a small business. They need to look at small businesses as well as the larger ones.

What we have done for FEMA, and specifically with the contracts we are putting in place ahead of disasters and the ones that we have for long-term recovery, we have actually put in significant small business requirements, localized small business requirements

that will come into play should something happen and they are activated, where if it is a larger company that has the contract, they have to give a large percentage of the work, anywhere from 50 to 75 percent of the work, to local businesses in the affected area.

Our goal is to get people working back in the area that are affected as opposed to a company coming in from halfway across the country to do the work. Simply put, for FEMA's needs, there are some things that FEMA needs to do that only large business has the capacity to achieve on a short notice. But what we have done is encourage them to utilize small businesses in that process.

Senator PRYOR. Right.

Mr. MARTINEZ-FONTS. Sir, if I can just add one comment on that. On the small business side, I agree with everything Mr. Bourne has said, but also the preparedness side of it is what really needs to be the key. I mean, there are so many businesses that are just so small that what they need to do is just have the right preparation, and through the Ready.gov, Ready Business type of outreach, we have been trying to get businesses to make sure that they have backed up their records, got a place to have follow-up plans. So really, the focus there, while I appreciate the question was really more on what happens in the aftermath—and by the way, our office held the first small business event in New Orleans after Hurricane Katrina—but really, it is an issue of preparedness that needs to be—more emphasis needs to be put on.

Senator PRYOR. Senator Akaka.

Senator AKAKA. Thank you very much, Mr. Chairman.

Mr. Martinez-Fonts, the Nation faces a very real possibility of a pandemic influenza outbreak which would affect the operations of everyone, large and small businesses, as well as communities, schools, and government and people, especially. In the event of a pandemic flu, private sector partners could serve as a powerful tool for tracking and locating employees, disseminating incident information, and coordinating response efforts.

Your written testimony discusses the Department's efforts to increase business owners' awareness of the importance of pandemic flu preparedness, business community planning and emergency response coordination. How is DHS incorporating private sector input and feedback into the Department's pandemic flu planning?

Mr. MARTINEZ-FONTS. Sir, if I could answer that question, I had the honor to go around the country last year with Secretary Leavitt and the Department of Health and Human Services representing Secretary Chertoff at their outreach on pandemic influenza. What that led to, the tour took in all 50 States as well as territories. I attended about 15 of them. There was a request for what I like to refer to as the two lanes in the pandemic issue. One is the medical side or the epidemiology of the disease. The other one is the critical infrastructure side of it.

HHS is clearly in charge of the epidemiology of it, making sure eventually that there will be a vaccine, that there are antivirals, that the hospitals are operating, etc. But those hospitals and the community isn't going to be able to operate without critical infrastructure.

So through a pilot program that we have done with the U.S. Chamber of Commerce and with a not-for-profit called Safe Amer-

ica, we have been going around the country, in addition to speaking to specific groups, and I happen to have a list, if you are interested, of all the outreach literally done. I didn't actually count them, but I would say it gets up to close to 100 between what we did with HHS and what we have done reaching out to both critical infrastructure and businesses of all sizes and making sure that they have made their plans, because unlike Hurricane Katrina, where as awful as that was, resources were able to be brought in from all around the country. In a pandemic influenza, if it looks something like the 1918 pandemic, it will hit the country equally all around and so there will not be very much shifting of resources around.

So we have an awful lot of lessons learned that have been shared in that. There is an excellent website that was started by HHS, but now 17 agencies are putting information on it, called PandemicFlu.gov. There is an infrastructure protection out of DHS, a program called Critical Infrastructure and Key Resources, Continuity of Operation Essential, which is available on the web. It is available on PandemicFlu.gov, and it really helps businesses, whether they are actually part of critical infrastructure or even if they are not, the types of preparations they need to do, because although much of the preparation that could be done for a hurricane or a flood is useful, in a pandemic, we are looking at a very extended period of time and we are really looking at not the destruction of the actual infrastructure, but having people just not be available.

Mr. ANDREWS. If I might add, one of the other initiatives that BENS has undertaken that relates to your question, Senator, is through their Business Force efforts, particularly in the State of New Jersey and in Georgia, they have run exercises utilizing the private sector for assistance in the distribution of the Nation's Strategic Pharmaceutical Stockpile. So using private sector resources both as facilities to help distribute it, using personnel within the private sector to help distribute the resources, which will probably overwhelm the capabilities of local government to do so.

So I think it speaks to the point that Mr. Ackerman made about the importance of practicing these. We need to do this more extensively across the country, but I think the lessons that have been learned in those exercises could prove valuable in a number of different regions.

Senator AKAKA. Thank you.

Senator Breaux, your written testimony states that the BENS Task Force recommended that Congress amend the Stafford Act and enact a nationwide body of disaster law to preempt the patchwork of State law in the narrow context of disaster response. The BENS Task Force report describes your recommendations in some detail. Has your task force developed a specific legislative proposal for a natural disaster law?

Mr. BREAUX. We don't have legislative language or a legislative proposal, Senator Akaka, but I think that what we have concluded is that the Stafford Act, which has served this country very well since Bob Stafford authored it a number of decades ago, was meant to help the Federal Government assist local and State governments, but the private sector really wasn't part of that mix at that time. I think what we are suggesting is that this Subcommittee

and the appropriate committees take the time, don't run through it and do it overnight, but take the time to look at what you all could do to improve the operational dictates of the Stafford Act and get local and State governments to have a plan that incorporates the private sector from the very beginning.

We have outlined some of the difficulties that private entities have had in responding to disasters, some of the legal and regulatory problems that they have had, some of the transportation problems that they have had, and if the Stafford Act could be amended to bring them into the planning process from the very beginning, require that FEMA grants go to States that have adopted a private sector plan into their emergency preparedness operations, I think those type of suggestions, I think that this Subcommittee could look at as potential amendments to the Stafford Act. Don't throw it out the window because it has worked very well. Just fix it up around the edges and it would be a real service.

Senator AKAKA. Thank you for that. I was interested in how far you have gone in that, because any kind of help we can get from you will certainly—

Mr. BREAUX. I do think that we have got a very talented staff over there and I think that they would be more than willing and able and very anxious to participate with your staff in the process of making those suggestions for you all to consider.

Senator AKAKA. Thank you very much. My time has expired.

Senator PRYOR. Thank you, Senator Akaka.

Let me follow up there, if I may, with Senator Breaux. You mentioned the national disaster law, which is a good concept for us to think about and put on the table and see if we can come up with something that makes sense. But do you think that part of that should include a good samaritan provision?

For example, when I was in the State legislature in Arkansas, we had a bill before us which I voted for that basically said doctors couldn't be sued—I can't remember exactly how it was structured—it was basically if they happened upon an accident scene or they were providing some free service. They couldn't be sued for malpractice for trying to help somebody.

I know Arkansas has other good samaritan-type laws and there are many other States that have some variation of those laws. But do you think that the national disaster law that you talk about should include some sort of good samaritan provision?

Mr. BREAUX. Yes. I think the short answer would be yes, with the caveat that obviously you just can't waive all the laws that protect citizens from being damaged by the negligence of someone trying to provide assistance or doing it in an incompetent manner.

But I think when you are dealing with a time of emergency, if providers of services know that they would be protected in those unique situations if they exercise their best judgment, that would be something that I think would be extremely helpful. It would encourage people to participate.

I mean, how many times have we heard people who have hesitated to participate in an emergency, even a small one, somebody collapsing on an airplane, "Well, I don't want to get involved." "I am a doctor. If I treat him, I may do the wrong thing. I will probably get sued."

I think that type of emergency protection would be very worthwhile. People could respond in those difficult situations. I mean, people may die if they don't, and yet they may not because they fear being sued. So in those narrow situations, exercising your best judgment, I think, should be encouraged and that would certainly do that.

Senator PRYOR. Mr. Ackerman, in your experience with Hurricane Katrina and other disasters in corporate America, have you had those same liability concerns in various contexts?

Mr. ACKERMAN. I think we do. Obviously, we worry about those exposures. What we have found, in general, is oftentimes business will go ahead and assume that risk, but it is never easy because one knows the exposure that is out there. So these situations do come up. Individuals, companies, managers, people have to make those decisions. I don't think that there is any given pattern to how it comes out, but I do think that people who are not risk averse generally follow that pattern, but then we have to worry about the litigation outcomes afterwards, so it is a constant issue.

Senator PRYOR. Yes.

Mr. MARTINEZ-FONTS. Mr. Chairman, if I could add, I was a banker for 30 years prior to joining the Administration, and since my last 5 years in government, I have been watching and I believe that liability issue will literally stop a private sector company in its tracks as they are concerned now. As Mr. Ackerman just said, many people will go out there and be very forward-leaning with it and will take the chance, but I have also seen a lot of cases where people have just sort of stopped and said, "I am not sure what it is going to do to me and so I am not going to go forward with it."

Senator PRYOR. It is a real concern.

Mr. Martinez-Fonts, if I can stay with you just for a moment. Last February, Secretary Chertoff told the Senate Homeland Security Committee that DHS needed an integrated Incident Command Center. I think you maybe mentioned this in your opening statement, but could you again give us a status report on this Incident Command Center?

Mr. MARTINEZ-FONTS. Sir, I am not sure I mentioned it in my statement, but we have a National Operations Center (NOC), where we have a common plan, a common operating picture that comes together and has the ability to now, for the Department of Homeland Security, bring together all of those incidents and is able to bring up to the Secretary's level all the information and then have it filter down to the right operational people within the Department.

Senator PRYOR. So do you feel like that Incident Command Center he referred to is in place?

Mr. MARTINEZ-FONTS. I think it is, if I am thinking of the right thing, sir. I would say, yes, that it is, and it has really become a much more robust program than anything we have had before.

Senator PRYOR. Has it been tested?

Mr. MARTINEZ-FONTS. It is tested very regularly, and not only have—I would say have they tested their own performance, but they have now performed on behalf of the Department in other external exercises and, therefore, in effect, tested themselves in the

ability to interact with the rest of the first responder community and the rest of the country.

Senator PRYOR. So it sounds like what Mr. Ackerman was talking about, you have done some practice with it, but have you also used it in disasters, yet, do you know?

Mr. BOURNE. I can answer that.

Senator PRYOR. Go ahead.

Mr. BOURNE. National Response Coordination Center, which FEMA manages, is actually a module, a node, a part of the National Operations Center. We routinely, with the National Operations Center, keep track of ongoing disasters and emergencies that happen across the country. There have been a number of incidents that have taken place, especially since Hurricane Katrina, on average, 50, 60 disasters a year of which we are in both FEMA's operations facility and the NOC are providing the Secretary with situational awareness on what is happening, helping to make resource allocation decisions, assisting us in obtaining additional information to help our operations on the ground. So there have been a number of declared events, Stafford Act events, in which the National Operations Center has been an integral part of our activities.

Senator PRYOR. Okay. And one last question for you, Mr. Martinez-Fonts, and that is, as I understand it, DHS has done some public-private initiatives and partnerships with the airlines, shipping, chemical industry. Are there lessons learned there that you can apply to other sectors and maybe expand on?

Mr. MARTINEZ-FONTS. Yes, sir. A very good example of what I had brought up earlier was the critical infrastructure. The industries that you just talked about are all critical infrastructures, and as you know, those are all under the direction of Assistant Secretary Bob Stephan. There are Sector Coordinating Councils, in effect, one Sector Coordinating Council for each one of the critical infrastructures, and that group is just constantly—it has two sides. It has a private sector side and a government side, Sector Coordinating Council, Government Coordinating Council. They are constantly testing and proving and providing information. Those lessons learned are then spread out between the Sector Coordinating Councils, between the Government Coordinating Councils, and among all of those.

An example was the Critical Infrastructure Key Resources Guide that I mentioned earlier for pandemic. That has been distributed widely because it just really is something that is very useful. In other words, if the largest of companies could do this kind of thing, what lessons can be learned or could be utilized and applied for a smaller company? And so that distribution has been very widespread, and yes, in fact, those lessons learned are being shared all across.

Senator PRYOR. Great. That is what we want to hear.

Dr. Andrews, let me ask you about—I believe Senator Sununu asked about EMAC and there has been some discussion about a Business Emergency Management Assistance Compact. Some people call it BEMAC. Is there such an entity now? Is there a BEMAC?

Mr. ANDREWS. There is not a formal BEMAC system across the country.

Senator PRYOR. Should there be, and if so, how do we structure that? Does it make sense to do it State-by-State, region-by-region, industry-by-industry? Tell us your thoughts on what a BEMAC might look like and how it should function.

Mr. ANDREWS. Well, the task force that I chair, we have looked very carefully at this, and again, trying to be as practical as we possibly can in terms of the recommendations that we make. Many of the ideas and, I think, elements of this have been outlined in the BENS report and it really starts with having in each of the States a Business Operations Center, that is, someone within the various critical—people within the various critical sectors who have been identified in advance, who understand the processes that are used by that State when an emergency occurs, and who will report either physically or will be in communications with the State's Emergency Operations Center when it is activated representing their sector.

If this exists across the country in the various sectors and requests are made through the EMAC system for resources that cannot be filled within the impacted State, then they would have reach-back into the other States that might be able to provide that source where in turn you would also have representatives from the business community.

It is an interesting situation, where there are some States, for example, North Carolina, where they do use private sector resources as agents of the State in out-of-state responses. And, in fact, legal opinion from, for example, the private medical community is that it is only under this structure that they can really respond out-of-state.

I think as part of a review of the Stafford Act, this might be something that we need to take a look at, because some States do have specific provisions that prohibit the use of private sector resources as agents of the State, whereas other States allow it. If there was some national ability where States could, in fact, use private sector resources as agents of the State, understanding the liability and reimbursement issues, I think it would be possible to formally align the business community with the EMAC system.

And again, given the fact that the EMAC legislation has been approved by all 50 State legislatures, I think this is something that continues to be a kind of linchpin that we need to build on. Right now, I see the system operating essentially in parallel with the EMAC structure, but NEMA and the State Emergency Directors are committed over the course of the next year to continuing to work with our task force to try to resolve any issues that remain.

Senator PRYOR. Thank you.

Mr. Bourne, as you well know, in February 2006, the White House released its report called "The Federal Response to Hurricane Katrina: Lessons Learned." One of those recommendations was to establish the system that allows for direct delivery of goods from private sector vendors to customers and, therefore, bypassing the need for storage sites, and other reports, think tanks, groups, etc., have made similar recommendations.

However, and maybe I misunderstand this, but my understanding is that FEMA has decided to rely more on forward-basing

of products in government-run storage sites. Do I misunderstand that?

Mr. BOURNE. No. Actually, while we do have a number of logistics centers across the country for certain commodities that we move very quickly into areas, we are actually looking at long-term, over the next year or so, developing a third-party logistics system where we are not the ones owning, storing commodities that would be used in various responses. We would have, essentially, a system where we would have access to those through contracts, pre-arranged third-party logistics management where the folks out there who do this all the time, whether it be the trucking companies, the Wal-Marts of the world, the Home Depots, etc., are the ones managing that for us with us having full visibility into where those commodities are and where they are going.

Our Logistics Management Directorate is taking an active look at this right now. There has been an assessment done on it. We are moving away from purely maintaining our own stocks of things. We always run into the issues of, is it available when we need it? How far do we have to move it? We want to shorten supply lines and the best way to do that is to tap the industries that have them in the areas that are affected, and that is the direction we are headed in.

Senator PRYOR. And let me ask about the TOPOFF 4 exercise. Can you tell me a little bit about that?

Mr. MARTINEZ-FONTS. TOPOFF 4 is the fourth of a series of Top Officials exercises that take place every 2 years. I believe it has now been rescheduled—I forget the exact date for this year, but I think it is October or so in the fall, and it is an exercise wherein something will happen, whether it is a—it could have been—during TOPOFF 3, we had some chemical agents being dispersed. It took place on the East Coast. It was in New Jersey. It was up in Connecticut, Rhode Island, and the like, and we actually exercise in place the events and coordinate with both the private and the public sector, State and local and everyone that is involved. So the coming-up event will take place in Seattle, Arizona, and Guam.

Senator PRYOR. So the private sector is involved in that?

Mr. MARTINEZ-FONTS. Yes, sir, they will be.

Senator PRYOR. And when Administrator Paulison testified before the House Homeland Security Committee on May 14, I think he had 13 pages of testimony, but he did not mention one time the private sector, as I understand his testimony. You guys probably weren't there. That just raises a concern in my mind that here you have the FEMA Director explaining to the House, explaining to the Congress different things that they are doing. I think he talked about the playbook, pre-scripted mission assignments, etc. But apparently during that testimony, at least in his prepared remarks, he didn't mention the private sector.

From your standpoint—I will just ask you, if I may, Mr. Bourne, do you think the private sector is sufficiently involved in, as they say, pre-scripted scenarios?

Mr. BOURNE. We are just beginning this relationship, quite frankly. We have done a lot of work. We have got a lot more to do. FEMA has been engaged in doing a reform top to bottom which involves a lot of moving parts. Never mind the fact that we have also

brought in programs that had not been in FEMA prior. So we are beginning this relationship. That is why we are bringing BENS and BRT and the Chamber together next week to further this relationship and figure out what other avenues that we can take.

We have spent a tremendous amount of time over the last several months in the rewrite process of the National Response Plan to take in private sector concepts and ideas as part of that writing process, and I think that the Subcommittee will see as we begin to roll that out in the next several weeks for comment that a lot of the—that there has been private sector involvement in that planning, in the document, but that much more needs to be done and we are embarked on that.

Senator PRYOR. Great.

Mr. BOURNE. One of the things I will just add to your prior question, if I could, our staff tells me that we are planning a logistics briefing next week and certainly will make that available to your staff.

Senator PRYOR. Great. Thank you.

In the Post-Katrina Reform Act, we mandated Regional Strike Teams. Are you familiar with those? Is the private sector involved in the establishment of those Strike Teams?

Mr. BOURNE. Not directly, and I will tell you why. The way the legislation was crafted and the way that we have had to build the teams, they are Federal responders. FEMA traditionally in its response puts out folks that are, quite frankly, it is a pick-up team in many respects in the past. They are folks in our regional offices and from headquarters that have other responsibilities day-to-day. They are formed into what they call Emergency Response Teams and then they are sent to disasters.

We are changing that model. We don't call them strike teams now. We are calling them Incident Management Assistance Teams. We are building them now, and they are going to be full-time Federal disaster experts working for FEMA. They are not going to be there to supplant local or State emergency responders or incident command. They are going to be that initial response. Their job is going to be to respond to disasters, and when they are not responding to disasters, to train, equip themselves, train and exercise with State and local governments.

Now, is there a role for a relationship for them with the private sector? Quite possibly. We are going to have to look at what that means, and I think the most effective way to achieve that is after we have developed a relationship between these teams and the State and local government emergency management folks and see how they want to see that interaction take place.

Senator PRYOR. I want to thank my colleagues and thank the panel for coming here today and answering a long list of questions that we have and thank you for your actions to prepare America to meet the next set of challenges in the world of disasters and response.

We are going to leave the record open for 2 weeks if colleagues want to submit written questions. If Senators do that, I would love for all of you to respond to those as quickly as possible. Additionally, several of you mentioned inserting your statements as part of the record. Those will be included in the record, or if any of you

on the panel have any documents or other items to add to the record, we will be glad to include those, as well.

So again, I want to thank you all for being here at our inaugural meeting of our Subcommittee and we look forward to working with you. Thank you.

[Whereupon, at 3:55 p.m., the Subcommittee was adjourned.]

PART II: PROTECTING OUR CRITICAL INFRASTRUCTURE

THURSDAY, JULY 12, 2007

U.S. SENATE,
AD HOC SUBCOMMITTEE ON STATE, LOCAL, AND
PRIVATE SECTOR PREPAREDNESS AND INTEGRATION,
OF THE COMMITTEE ON HOMELAND SECURITY
AND GOVERNMENTAL AFFAIRS,
Washington, DC.

The Subcommittee met, pursuant to notice, at 2:03 p.m., in room 342, Dirksen Senate Office Building, Hon. David Pryor, Chairman of the Subcommittee, presiding.

Present: Senator Pryor.

OPENING STATEMENT OF SENATOR PRYOR

Senator PRYOR. Let me go ahead and call us to order. Thank you all for being here. I thank the members of the public who are in the back there, as well. We appreciate your interest.

Welcome to the Ad Hoc Subcommittee on State, Local, and Private Sector Preparedness and Integration. I want to welcome everyone here today and thank you for taking time out of your busy schedules to be here.

This hearing is a continuation of an ongoing dialogue we are having on the Subcommittee and here in the Senate with the private sector focusing on the importance of making sure that the government and the private sector are working together to protect our critical infrastructure.

Simply put, critical infrastructure is defined as capabilities and services that secure our country and make it livable. We all know this, but it includes everything from highways to communications to financial services to electricity and we use it to accomplish everything we do throughout the day. For example, we wouldn't be here today if we didn't all rely on critical infrastructure to get here and to utilize what we have here in this hearing room even.

Critical infrastructure assets are so interconnected that one accident or natural disaster could potentially cause a massive upheaval. The nuclear reactor accident in Chernobyl, Ukraine, for instance, exposed 6.6 million people to radioactive fallout and forced the evacuation of almost 400,000 people. In this country, Hurricane Katrina damaged oil refineries and spiked gas prices across the country. The disaster also disrupted Internet access, clean water supplies, telecommunications, and on and on and on.

Because disruption of our critical infrastructure would cause mass chaos and fear, these systems are prime targets for terrorists.

In early May of this year, the FBI and an attentive store clerk stymied an attempt by six men to "kill as many soldiers as possible," at Fort Dix Army Base in New Jersey. The men were in the process of making bombs and accumulating weapons. Once their plan was fully developed, they intended to storm the base, firing on and bombing our men and women in uniform.

Just last month, authorities foiled a terrorist plot to blow up JFK International Airport, its fuel tanks, and a jet fuel artery. Terrorists are focused on critical infrastructure and they understand how critical it is in the United States that we keep those things operational, even under adverse circumstances.

In this Ad Hoc Subcommittee, we are moving into a new era in terms of homeland security and national security. These terrorist plots that I have been talking about are living proof that extremist groups want to try to inflict pain on our citizens and on our economy and they are trying to do as much damage as they can to our country and they think they know how to do it.

For all these reasons, it is crucial to have an effective, well thought-out plan for protecting our infrastructure. Now, last year, the Department of Homeland Security released a plan called the National Infrastructure Protection Plan (NIPP). The NIPP was to set out a standard for industries to identify and prioritize critical infrastructure assets. It required each of the 17 critical infrastructure sectors to submit a plan dealing with the unique protection challenges that industry faces, and we have a chart here with those sectors listed.[1]

So for our efforts to be effective, we must make sure that both government agencies and the private sector are involved in creating the protection plans. In our hearing today, we will review the process of creating the plans, discuss the challenges and successes in public-private partnerships, and look at how the overall effort contributes to preparedness.

With that in mind, understand that today is a very busy day in the Senate. We have DOD authorization on the floor and there are lots of amendments and lots of Senators have committee hearings, so we don't know how many Members will be able to attend, but certainly when colleagues show up, we will try to accommodate them and get them in and let them ask questions and move on to their next stop.

What I would like to do is go ahead and introduce our panel. We have your backgrounds already and we will submit those for the record. Each of you will have 8 minutes to give an opening statement. If you want to just submit that for the record and summarize, that is up to you.

Let me just run through the panel very quickly and just say a few words about each person and then I will open it up and let you all give your opening statements.

Our first witness will be Bob Stephan. He is the Assistant Secretary for the Office of Critical Infrastructure Protection at the U.S. Department of Homeland Security. He is responsible for DHS's efforts to catalog our critical infrastructure and resources

[1] The chart referred to appears in the Appendix on page 227.

and coordinate risk-based strategies to secure them from terrorist attack or natural disasters.

Eileen Larence will be the second witness. She is the Director of the Homeland Security and Justice Issues Division at the U.S. Government Accountability Office. She manages investigations, issues reports, and makes recommendations, and handles Congressional requests for work on homeland security issues.

And then Ken Watson will be third. He is Vice Chairman of the Partnership for Critical Infrastructure Security. He established the Critical Infrastructure Insurance Group with the goal of driving Cisco's contribution to the security of worldwide critical infrastructure.

So Mr. Stephan, if you would lead off for us.

TESTIMONY OF COLONEL ROBERT B. STEPHAN,[1] ASSISTANT SECRETARY FOR INFRASTRUCTURE PROTECTION, U.S. DEPARTMENT OF HOMELAND SECURITY

Colonel STEPHAN. Mr. Chairman, thank you very much for the kind invitation to appear before you today. I sincerely appreciate the opportunity to address you on the role of the Department's Office of Infrastructure Protection and ensuring robust coordination with the private sector as we work actually together as a team to protect our Nation's critical infrastructures from terrorist attack and also enable their quick recovery in the wake of a terrorist attack or a natural disaster because we have another terrorist to deal with in our mission space and she is called Mother Nature.

My staff and I are keenly aware of the importance of fully integrating and working with our private sector partners across our mission space as well as with our State and local government partners. As a point of departure for your team, it is important that we note that the vast majority of our Nation's critical infrastructures, about 85 percent or so, those are owned and operated by the private sector in some way, shape, or form. Hence, our comprehensive work with the private sector represents a very key component of our national protection network as well as our national information sharing network.

Both the Congress and the President of the United States have recognized that full support, cooperation, and engagement of government and private sector partners at all levels is required to prevent terrorist attacks, mitigate natural disasters, restore essential services after an incident, and to generally maintain the American way of life.

Our partnership with the private sector spans the diverse spectrum of the 17 sectors that are identified in Homeland Security Presidential Directive No. 7. You have those catalogued there in your chart. This partnership also extends very importantly in a boots-on-the-ground-type construct to high-risk communities across the country, where my staff and I have put a great deal of focus and effort to bring together Federal, State, and local government partners and the private sector to engage in vulnerability assessments, security planning, information sharing, best practices exchanges, risk reduction and incident management activities.

[1] The prepared statement of Colonel Stephan appears in the Appendix on page 104.

Since the creation of my office in March 2003, our mission has been very clear. Our overall approach focuses on establishing and sustaining a risk-based unified program to protect and enhance the resiliency of our Nation's infrastructures. The key to this approach is a layered defense constructed of physical protection, cyber security, and resiliency within the sectors as tailored to the requirements of each of those sectors. This again, sir, is a long-term effort that involves a comprehensive government and private sector engagement inside and outside of regulatory space at various levels across our national risk landscape.

The private sector has made significant investments to strengthen both physical and cyber security to boost resiliency, increase redundancy, and develop contingency plans since the September 11 attacks. Of equal importance, State and local agencies have stepped up to this mission plate and have strengthened infrastructure preparedness within their jurisdictions. Supporting these efforts, in one example, DHS has provided nearly $2 billion in infrastructure-targeted risk-based grant funding over the past several years, to include $445 million this year.

Our partnerships across various levels of government and with the private sector form the operational core of our National Infrastructure Protection Plan—sir, we do affectionately refer to that as the NIPP, and thank you for highlighting that—and, as well, the supporting 17 Sector-Specific Plans (SSPs), in each of the sectors. Through the NIPP and these supporting plans, we now have a unified national game plan and an ever-expanding arsenal of tools to implement our mission.

The NIPP base plan establishes the overall risk-based approach that defines the unified way we are going to protect the enhanced resiliency of our critical infrastructure sectors across the board. Organizationally, the heart of the NIPP is bringing people together in some kind of construct? It is akin to bringing good Super Bowl teams to the playing field at the end of football season. Establishing Sector Coordinating Councils on both the government side of the house and on the private sector side of the house, bringing the right people to the table in a legally protected framework to get the job done, whether it is policy recommendations, planning, looking at risk assessment methodologies, planning for incidents and actually conducting incident management operations.

Within the NIPP, the NIPP partnership models encourages private sector owners and operators to establish Sector Coordinating Councils as a principal entity for coordinating with the government across a wide variety of issues. These entities are self-run and self-governed and their specific membership varies from sector to sector, including owners and operators, associations, and other entities, corporations, or individual companies, both large and small. The finalization and release of the NIPP Sector-Specific Plans used this framework in terms of its development and will be an essential piece of implementing and integrating those plans across the 17 sectors.

Developed under the umbrella of the NIPP partnership model, the Sector-Specific Plans represent adaptations of the NIPP baseline risk analysis and risk management framework, its governance structure and information sharing protocols, as tailored, once

again, to the specific needs and requirements of each of the 17 sectors, which are very different in and amongst themselves.

This undertaking represents the very first time that government and private sector entities have come together on such a large scale across every sector of the economy to develop joint plans to better protect and ensure the resiliency of our critical infrastructures against both terrorist incidents and natural disasters. Each plan contains concrete deliverable milestones and timelines that define the road ahead for each of these sectors.

In a series of parallel undertakings, we are leveraging the NIPP sector partnership model and coordinating council structure to finalize a comprehensive annex to the National Response Plan that deals with infrastructure protection and restoration; to develop sector-specific guidelines for pandemic influenza preparedness; establish infrastructure protection research, development, modeling, simulation, and analysis requirements; and building a National Infrastructure Protection Awareness and Training Program, to include exercises such as the upcoming TOPOFF Officials 4 exercise, which will be conducted in October of this year.

Our partnership framework enables more progress in another important area, information sharing, where we use the NIPP partnership framework to share information of a risk-based nature on a day-to-day basis that includes operational information, situational awareness of incidents that are occurring across our infrastructure sets around the country every day, and we use that same incident management information sharing network to collaborate and integrate with one another during crisis, incidents, or emerging threat scenarios.

Another important advancement in our relationship with the private sector is the establishment of our Homeland Infrastructure Threat and Risk Analysis Center, or HITRAC. This is an infrastructure and intelligence fusion center that we operate in a joint partnership with Charlie Allen, the Assistant Secretary for Intelligence and Analysis at DHS. Through this center, we provide access to classified information. We enable members of the private sector leadership to obtain security clearances to the tune of about 900 so far across the sectors and using the tear-line concept are able to share very broadly important emerging threat products with the private sector at a tactical and strategic level.

Through the HITRAC and our National Infrastructure Coordinating Center, which maintains an operational status or pulse of the Nation's infrastructure on a day-to-day basis, or private sector partners receive real-time threat situation and status information and analyses, which is in turn used to inform security and operational planning, resource investments, and key risk mitigation activities.

Coordinating with other key stakeholders through our partnership model is fundamental to the success and it has also been a key enabler to allow us to push out the door very important boots-on-the-ground activities that are having a very noticeable impact in terms of improving our security posture across the private sector infrastructure landscape. Through our comprehensive review program, we provide a structured joint analysis, Federal, State, and local capabilities, private sector capabilities needed to enhance the

security of our highest-risk national infrastructures. Today, we are virtually through, and we will be through in September, walking across the chemical sector and the nuclear energy sector in terms of a comprehensive review process, bringing lots of inside and outside defense equities to the table.

Through our Buffer Zone Program, we have a DHS-administered grant approach that is designed to assist local law enforcement and private sector critical infrastructure owners and operators increase security within the buffer zone, or the area outside a facility that can be used by an adversary to conduct surveillance or launch an attack. Through this process, we have completed more than 2,200 individual site visits in locations across the United States, pushing approximately $190 million out the door to State and local law enforcement to provide connectivity to specifically identified critical infrastructure facilities and boost their reinforcing capability for prevention through protection to response and recovery.

Our Protective Security Advisors represent a cadre of 78 folks right now in place across the country in key urban areas, rural areas of the country, places where we have a nexus of population and critical infrastructures. These Protective Security Advisors (PSAs), foster partnerships, facilitate collaboration, conduct vulnerability assessments, facilitate training and exercise programs, provide general situational awareness back to me on a day-to-day basis. They have conducted about 15,000 liaison visits with private sector owners and operators over the past 2 years and they are my first boots on the ground in terms of the infrastructure protection Federal mission subset during any incident, and they have a very comprehensive and solid list of Rolodex contacts across the Federal, State, and local community and the private sector community in their geographic areas of responsibility.

Through them and others, we have conducted soft target awareness courses and surveillance detection training programs across the country. The soft target piece is a week-long course that provides private sector owners and operators and security personnel with a venue to receive and share baseline terrorism awareness, prevention, and protection information and is intended to enhance individual and organizational security awareness. Our surveillance detection course provides a guideline for mitigating risk to infrastructures by developing, applying, and deploying protective measures in the creation of a surveillance detection plan within facilities such as shopping malls, arenas, stadiums, public access, and gathering sites. We have conducted 284 surveillance training awareness courses across the country as well as an additional increment of the same number of our soft target awareness training packages.

Our TRIPwire program, bombing prevention, is highlighted by the recent events in London and Glasgow, a very important part of our day-to-day business. This is an online web-based tool that provides the latest and greatest information to bomb squad, private sector security folks, law enforcement officials across the country in terms of terrorist tactics, techniques, and procedures relative to IEDs, VBIEDs, and maritime-based improvised explosive devices. To this date, we have got about 40 Federal departments and agencies, 28 military units, 365 State and local law enforcement agencies, and 35 private sector companies hooked into this website, and

in the last year since it has been operational, we have had nearly four million site hits.

Finally, with respect to the demands of incidents caused by Mother Nature, we have put into place through our Protective Security Advisor Network out in the field and through infrastructure specialists here at the Department headquarters and in cooperation with our national ops center and FEMA headquarters a very robust set of experts that are manning watch 24/7 and are prepared to respond and organize a team of specialists around any type of incident that involves the downing of our infrastructures, that would involve follow-on security assessments, restoration and recovery operations, or any type of assistance or information sharing requirements that we need to bring to the table.

In terms of my remaining time with you today, looking toward the future, we are finalizing our office's long-term strategy for continued program growth and evolution. We are finalizing our 2008 to 2013 strategic plan—I hope to have that done within the next couple of weeks—that identifies a very significant number of primary goals essential to implementing our national mission and continuing to build out this very important public-private sector partnership framework. This effort is being conducted in tandem with our sector annual reporting process under the National Infrastructure Protection Plan. Our goal is to continue our risk-based approach to infrastructure protection, tailored again to the needs and requirements of the individual 17 sectors. As we move into the future, the NIPP partnership framework and the tens of thousands of security partners across the public and private sector that it brings to the table will continue to drive our national approach.

Certainly, no one can predict the future with 100 percent accuracy, but certain things are a given. Technology, the way in which owners and operators do business, and their supply chain dependencies and interdependencies will certainly evolve, and vulnerabilities and consequences will change accordingly. We can also count on our risk calculation changing over time.

Another fact is very clear. We face a very clever, flexible, patient, determined terrorist adversary. The path forward provided by the NIPP, the Sector-Specific Plans, and the partnership framework allows us to act collaborative as together we adapt to a very dynamic risk environment, a very dedicated and very ingenious enemy through a national unity of effort that we have begun to build and will continue to build out over time.

Success over time means making commitments and following through on them. We will approach our collaborative implementation of the NIPP and the SSPs with this in mind and continue to refine and enhance our solid partnership with the private sector, State and local governments.

I will leave you with one more important observation. The more we utilize the sector partnership model, the stronger and more effective it gets. We will continue to incorporate lessons learned, strive to constantly improve and adapt our partnership, communications, and coordination with the changing times and risk landscapes at the national level. Continued support of our focused activities in concert with all of our partners will help ensure our Nation's preparedness in my mission area.

Sir, thank you for this important opportunity to discuss the infrastructure protection mission area, and the public-private sector partnership framework that truly lies at its core. I would also like to thank you for your continued support and the support of this Subcommittee and the larger Committee of which you are a part for your dedication to the success of this vital component of our overarching homeland security mission, and I would be happy to answer questions following my colleagues. And sir, thank you for your time today.

Senator PRYOR. Thank you.

Our second witness, whom I introduced a few moments ago, is Eileen Larence. I suspect that I have mispronounced your name.

Ms. LARENCE. That is right.

Senator PRYOR. Is that right?

Ms. LARENCE. No "W".

Senator PRYOR. OK, thank you. Go ahead.

TESTIMONY OF EILEEN REGAN LARENCE,[1] DIRECTOR, HOMELAND SECURITY AND JUSTICE ISSUES, U.S. GOVERNMENT ACCOUNTABILITY OFFICE

Ms. LARENCE. Mr. Chairman, I appreciate the opportunity to discuss the results of GAO reviews of the Department of Homeland Security's efforts to ensure the Nation's most critical infrastructure, from power plants and health care workers to the Internet, is protected from terrorist attacks and disasters, a daunting and complex challenge as Hurricane Katrina demonstrated and you pointed out in your opening statement. It is also an important mission, as DHS estimates infrastructure influences about 50 percent of our GDP, and as my colleague mentioned, about 85 percent is owned by the private sector, meaning DHS must depend on partnerships with this sector to voluntarily pay for added protection. DHS also recognizes the Nation cannot afford to protect everything, so it has devised a risk management model for infrastructure investments, an approach GAO generally endorses.

As you pointed out, sectors were to create Sector-Specific Protection Plans. These plans were due to DHS by the end of December and released on May 21 of this year, and sectors recently submitted status reports on where they are against these plans to DHS. In terms of these plans, it is important to realize that they are separate from emergency response plans. We also found that they tend to be what we would call plans to plan, meaning that they describe how or what processes the sectors are going to use to identify their critical assets and resources, assess their vulnerabilities and risks, prioritize their resources, and select protective measures for them. And while owners and operators may to date have implemented protective measures for some of their individual assets to maintain business continuity or to comply with existing regulations, sector plans are to go beyond individual assets and take a more comprehensive national look at vulnerabilities and gaps across the sectors.

GAO has reviewed the stand-up of the Coordinating Councils, the NIPP, and nine of the sector plans, as well as interviewed the

[1] The prepared statement of Ms. Larence appears in the Appendix on page 115.

chairs of each council, and has drawn several findings from this work.

First, while sector plans are very useful to DHS in providing a consistent baseline, sectors had mixed opinions about the value of the plans and some were not as detailed and complete as others, which could limit their usefulness.

Second, sectors have faced several challenges moving forward as plans and implementation evolves.

Third, it appears that relatively few sectors are close to completing all of the systemic steps called for in the NIPP and will continue to evolve, as well.

To further elaborate on each of these points, the sector plans are useful to DHS by providing it a baseline and consistent approach to protection, and a number of private sector representatives said that developing the plans was helpful for providing collaboration, information sharing, and common strategies. But for several other sectors, ones that were more mature, more homogeneous, or regulated, the plans are not as useful because these sectors had prior plans they were already implementing, such as in response to the Y2K scare, or because they did not think the private sector had been sufficiently involved in the process.

While all the plans met DHS guidance and NIPP requirements, the comprehensiveness and potential usefulness of the plans that we reviewed were also mixed. They all included protection goals and objectives and sector intentions for assessing, prioritizing, and protecting assets. But the plans varied in the extent to which they: First, discussed protective measures in detail, since some sectors were not ready to do so or chose not to; second, recognized how sectors depended on each other, such as for electricity, telecommunications, or water to continue operations, and laid out these dependencies in their plans and in implementation; third, comprehensively assessed not only their physical assets, such as buildings, but also their cyber and human assets, a gap that could deter sectors' readiness; and fourth, discussed possible incentives they could use to encourage private sector protection efforts, even though sectors depended on such efforts.

And while plans acknowledged the need for metrics to determine how much protection we are achieving, some are going to rely on qualitative measures of progress, such as tests accomplished, instead of outcome measures of protection achieved. We recognize that assessing outcomes will be very difficult, but as you know, measures drive performance, so addressing this and other gaps in the plans will be important moving forward.

As to our second finding, most private sector representatives spoke positively of their lead Federal agencies, including DHS, and the support provided, especially contractor support, but to varying degrees identified some challenges that they face: First, dealing with DHS reorganizations, staff turnover, and lack of expertise about some sectors; second, getting full council representation for some sectors that have a widely diverse membership, such as the health and agricultural sectors; third, having infrastructure that was primarily systems, networks, or people rather than buildings, and this complicated their planning, and according to the IT sector

representatives, also complicated qualifying for some of the grant programs, as well.

Another challenge was getting State and local players involved, in part because of the costs and time commitments, even though they are critical to protection efforts, and also, getting buy-in to the plans from all individual owners, operators, and private sector members. So marketing these plans will be important. This will also help to ensure that the plans don't simply sit on the shelf. And a final challenge was private sector reluctance to provide DHS with information on assets and vulnerabilities for fear that their proprietary information would not be protected, including from possible terrorists, or they would lose competitive advantage or face litigation.

As a result, most sectors still rely on their own voluntary information sharing advisory councils to share information and we are optimistic about the Critical Infrastructure Protection Advisory Council DHS initiated because it provides for closed meetings with the private sector. But others were still cautious about using DHS's program to protect critical infrastructure information and we had identified such reluctance in a report last year and proposed recommendations for improvements, and also using DHS's Homeland Security Information System because it lacks certain security features that were important to the private sector.

As for our last finding, according to the sector plans we reviewed and representatives we contacted, it appears that only a few sectors, especially more mature ones, are relatively far along in completing all steps in the sector-wide NIPP process, and several newer sectors, such as health care, were still in the early stages. The recent status reports that the sectors submitted to DHS may give us a more accurate picture of this progress.

DHS has made a lot of progress and has opportunities to promote this progress going forward. For example, it could target its support to the sectors that have made less progress. It can ensure that the critical gaps in the plans and the challenges we discussed are addressed. It can help sectors market these plans to get by in an implementation. It can streamline its review process in the future and provide the private sector more time for input, a problem a number of the private sector representatives identified in speaking with us.

Maintaining momentum and timelines for implementation will also be important. Continued Congressional oversight, such as assessing sector status reports to determine progress, assessing the threat information and risk assessments that sectors use, since they drive the investment decisions, and what sectors have achieved with grant funding can also provide momentum and GAO stands ready to support this oversight.

Finally, longer-term policy questions can include, does DHS have enough leverage to ensure the private sector will meet protection goals? Can we rely on market incentives or do we need other incentives, such as more targeted funding, tax incentives, or innovative R&D investments? Who will pay for any gaps between protection the private sector is willing to fund and any added protection needed to meet national security goals? And are we focused on the right goal, protection versus resiliency? Some in the private sector argue

the end game should be resiliency, which means how quickly can operations be restored after an incident, rather than protection, which they characterize as adding more guns, guards, and gates, because resiliency is measurable and perhaps more affordable. What is the right balance between these two goals?

This concludes my statement and I would be happy to answer any questions. Thank you.

Senator PRYOR. Thank you. Ken Watson.

TESTIMONY OF LIEUTENANT COLONEL KENNETH C. WATSON, (RETIRED),[1] VICE CHAIRMAN, PARTNERSHIP FOR CRITICAL INFRASTRUCTURE SECURITY, AND SENIOR MANAGER, CRITICAL INFRASTRUCTURE ASSURANCE GROUP, CISCO SYSTEMS, INC

Mr. WATSON. Mr. Chairman, thank you for inviting the Partnership for Critical Infrastructure Security (PCIS) to participate in today's hearing on America's private sector preparedness to protect our critical infrastructure.

The NIPP designated PCIS as the private sector cross sector coordinating council for protecting critical infrastructure, but in fact, we have been fulfilling that role for the last 8 years, since we formed in 1999. Our council consists of the Sector Coordinating Councils (SCCs), the private sector components of the designated critical infrastructure sectors. Most of the sectors have also established Information Sharing and Analysis Centers (ISACs), to manage the daily information sharing needs of the sectors.

In October 1997, the President's Commission on Critical Infrastructure Protection published its seminal Critical Foundations report, which identified two irreversible trends: Increasing privatization of critical services; and increasing migration of core business and government operations to networks, including the Internet. The Federal Government called for a public-private partnership and we responded by founding the PCIS in 1999 in response to that call.

We have made tremendous progress. I believe we are on a very solid path and the Nation's critical infrastructure is far more resilient to potential attacks or natural disasters than we were 8 years ago.

The PCIS Business Plan identifies four broad goals, each with its own objectives and metrics: First, partnership leadership on critical infrastructure issues and policy that reflect the consolidated all-sector perspective; second, cross-sector leadership in cross-sector interdependency issues; third, sector assistance to increase the value to the sectors and the SCCs; and fourth, PCIS effectiveness, improving the organizational effectiveness and value of the PCIS itself.

Our members see value in understanding issues common to multiple sectors, unique challenges or solutions from a single sector, and the ability to jointly approach DHS and other government organizations. In addition, because of our sector-specific subject matter expertise, the National Infrastructure Advisory Council, or NIAC, calls on us from time to time to help develop policy advice for the President. Two notable recent efforts studied pandemic vac-

[1] The prepared statement of Mr. Watson appears in the Appendix on page 140.

cine prioritization for critical infrastructure protection workers and issues surrounding public-private sector intelligence coordination.

Chief among our recent successes is the development of the NIPP and its 17 Sector-Specific Plans. This level of collaboration would have been impossible without the Critical Infrastructure Partnership Advisory Council framework provided by the Congress in the Homeland Security Act of 2002 and implemented by Secretary Chertoff more than a year ago. This CIPAC framework allowed us to work side-by-side with our government counterparts to write these plans. This collaboration improved the NIPP's approach to risk management. The initial DHS draft proposed a bottom-up approach for all the sectors which focused on physical assets. After considerable engagement between DHS and functionally-based sectors, such as electricity, IT, and communications, the NIPP Risk Management Section evolved to accommodate top-down risk management models, permitting multiple approaches.

Developing the Sector-Specific Plans (SSPs), was not a perfect process. Most sectors were pleased with the collaboration of their sector-specific agencies, but for others, a learning curve still remains. I see these as growing pains as all partners embrace the new framework.

The list of sector successes is long and growing. My written testimony highlights six sample success stories and I encourage you to review them at your earliest opportunity. For example, in the financial services sector, several Regional Partnership Councils have formed, allowing members to collaborate on disaster management matters with Federal, State, and local partners. Meanwhile, the rail and water sectors have begun meeting quarterly with key intelligence personnel to build trust, increase knowledge, and raise awareness. Using a competitive DHS grant, the commercial facilities sector created a training course to help managers of stadiums, arenas, performing arts centers, and convention centers to implement a DHS web-based security awareness and vulnerability assessment tool.

Removing barriers to private sector participation is a key initiative of DHS and the PCIS. The Subcommittee asked me to comment today on three specific areas of concern: First, issues of competitive advantage; second, fear of sharing sensitive information; and third, worries the partnership might exclude smaller operators.

I understand competition is cited frequently as a barrier to partnership, but I believe Greg Jones, the Chief Administrative Officer for Greenberg Traurig, LLP, summed it up best when he wrote recently, "We are competitors, not enemies." The same holds true for the collaborative approach embraced by the SCCs and the ISACs.

Regarding sharing sensitive information, we work closely with the Protected Critical Infrastructure Information Program Office (PCII), and the Information Sharing Environment (ISE), under the CIPAC framework to develop a simplified, rational approach to protecting information. As long as statutory protections for this information remain, the PCII Program should function within the newly-proposed Controlled Unclassified Information (CUI), environment.

Despite these efforts, some sectors still have serious and legitimate concerns. First, sectors are unclear about what sensitive in-

formation DHS needs. Second, sectors worry this information might be disclosed publicly, making it available to competitors or used in litigation.

SCCs include all relevant trade associations, a provision we insisted upon and DHS incorporated into the CIPAC framework to ensure inclusion of smaller operators. The food and agriculture SCCs, for example, has 119 separate entities representing the entire sector, from farm to table. The financial services SCCs has 34 associations and companies representing banks, brokerages, and insurers. In addition, Homeland Security Assistant Secretary Bob Stephan and others regularly travel around the country encouraging companies and associations to join their SCCs and ISACs, and we appreciate that.

Finally, please allow the PCIS to make a few suggestions that we, its members, feel would enhance the partnership and improve the ability of the United States to manage exceptional events. First, let the partnership mature. We have accomplished a great deal with DHS since its inception and even more since Secretary Chertoff exercised the Section 871 exemption to create CIPAC a year ago. While we welcome Congressional involvement, we must continue building a trusted environment that allows us to work freely with our government partners on sensitive safety and security issues. Moving forward, we would be happy to work with you as you consider standards and risk assessments.

Second, the PCIS asks you to help us educate all Federal partners about the nature and value of this partnership because it has not been executed uniformly across all sectors. Some in the Federal Government still fail to understand the model's merits. Many we work with in the DHS IT and Communications Operations Group and the Partnership and Outreach Division embrace the structure, but the farther you travel from those offices, the less understanding and appreciation of the sector partnership framework you will find.

Third, it is time to review the National Response Plan to include more proactive private sector participation in response actions. This is crucial in the cyber dimension, as PCIS considers all cyber incidents international by default. The private sector has multiple collaborative mechanisms to deal with significant cyber incidents. Many Internet service providers, for example, collaborate through the informal "nsp-sec" community. Multiple public and private sector incident response teams also belong to the more formal Forum of Incident Response and Security Teams (FIRST). These two organizations are really the global cyber first responders. In turn, the NRP should direct proper authorities to these and other like-minded organizations during a cyber incident of national significance.

Finally, the government must do a better job of sharing timely and useful information with the private sector. It is often difficult to determine exactly who needs to know sensitive information, but this partnership framework includes enough trust to err on the need-to-share side of the equation. Complex interdependencies, a lack of sector familiarity, and complex collocation of assets argue for a proactive sharing of alerts and warnings with the PCIS and the relevant ISACs. Many ISACs can transmit and store classified

material and many sectors have cleared individuals who can be trusted with sensitive information.

That concludes my remarks. Thank you again for the opportunity to be with you today on behalf of PCIS. I would be happy to answer any questions you have.

Senator PRYOR. Thank you. Mr. Watson, let me start with you, if I may. Just by way of background, tell me a little bit about your organization, the Partnership for Critical Infrastructure Security. I think you said it started in 1999. Why did it start? How does it work?

Mr. WATSON. The way it started, as you remember, the President's Commission on Critical Infrastructure Protection (PCCIP), or the Marsh Commission, reported its Critical Foundations report on the vulnerability of critical infrastructures and a plan forward in October 1997. The government responded with PDD–63, Presidential Decision Directive 63, in May 1998, which created a lot of government organizations including the CIAO, the NIPC, and a few others that were scattered around the Federal departments.

At the time, the Critical Infrastructure Assurance Office (CIAO), was in the Department of Commerce. The Department of Commerce put out a call for public-private partnership because that was the view of the Marsh Commission, that the only path forward because of these irreversible trends that I mentioned was public-private partnership. We responded by calling, I think over 200 companies to come to the table to form the PCIS, and our first meeting was actually in the Windows on the World restaurant at the top of the World Trade Center in December 1999. Since then, we created committees to look at research and development, information sharing, public policy, and any other areas that might be important to all the sectors or multiple sectors and began to coordinate with the Federal Government.

When DHS was formed, all of the offices that were dealing with critical infrastructure assurance moved into the Department, so we had a single face now to work with—to coordinate most efforts across the sectors. Now, we understand that many of the sector-specific agencies are not in DHS. DHS has the overall coordination role and we are comfortable with that. For example, the financial services sector had a long relationship with the Treasury Department and they want that to continue and we support that, and similar relationships exist for the other sectors.

Senator PRYOR. OK. And you have been asked to help coordinate the various sectors. What is your role there?

Mr. WATSON. Currently, I am the Vice Chairman of the PCIS. I am also on the Executive Committee for the IT Sector Coordinating Council.

Senator PRYOR. You obviously work very closely with DHS. Is there an arms-length relationship with DHS? Are you independent of them?

Mr. WATSON. We are very independent. At first, the funding model was donations from founding member companies. We got away from that because we believed that the business model that included payment of dues was exclusive and eliminated some of the smaller players, and so we eliminated the dues requirement. DHS stepped up to the plate after they were formed to help provide ad-

ministrative support as long as—and we made sure that they couldn't have access to private sector-only information, but if they wanted to provide information, that is what we are still doing admirably now. They support us in terms of coordinating conference calls, printing, organization support, meeting support, those kinds of things, and that relieves us of the burden of a lot of expenses.

We do have a Board of Directors and we pay for our own Directors and Officers insurance and our own budgeting, but it is so minimal that it is not a burden to anybody that would like to participate.

Senator PRYOR. Great. Now, let me ask, you mentioned in your testimony about the trust level with the private sector and the government, and I understand that sometimes the government is very reluctant to share classified information. Sometimes the private sector is very reluctant to share some of their proprietary information. I understand that. But what is the best way to balance national security and the need for the interested parties to be fully informed and have all the information they need? Do we have that balance yet? What do we need to do to improve that?

Mr. WATSON. We are making a lot of progress. We are not completely there yet. I think that the effort of the information sharing environment is a good one. It is not mature yet. We haven't really defined whether PCII will work within the framework. We think it will, but it hasn't been tested yet. Now, this is the ability to share sensitive information with the government. The private sector would like to share information with the government because the government has a role in helping us protect ourselves and the country from attacks and natural disasters.

On the sharing of sensitive government information, including classified information, HITRAC is a step in the right direction. It is the Homeland Infrastructure Threat and Risk Analysis Center—the DHS fusion center that brings in all of the threat and law enforcement information, and they have opened up HITRAC to private sector participants, which we think is a very positive step.

Now there is an opportunity to get private sector expertise in the door to help train government analysts on what is important and what is not important, so we are making progress, but there is more to do.

Senator PRYOR. Let me ask, I want to get to you in just a moment, but let me ask while I have you, Mr. Watson, there are 15 national planning scenarios that cover a wide range of disasters—earthquakes, floods, cyber attack——

Mr. WATSON. Right.

Senator PRYOR [continuing]. Pandemic flu, etc. To the layperson, it seems that we are covering the waterfront there, but is there anything that you think we are missing? Are there any scenarios that we really haven't thought of or something that might fall in the gaps that we are really not preparing ourselves for?

Mr. WATSON. That list of scenarios is pretty thorough. They are also plugged into the National Exercise Program, either one at a time or in combination, and I think that is the right thing to do. It is going to take an awful long time to get through all 15 if you do them one at a time. I think the nightmare scenario would be a large physical attack in combination with a cyber attack that dis-

ables the emergency response. That is the one that keeps us up at night. So if we could exercise that and make sure that the first responders—firefighters, police, emergency medical, and local government decision makers—work through the degraded communication that would happen in those kinds of things and had alternate means of communications planned in advance, we would be much more resilient to that kind of a combined attack.

Senator PRYOR. Let me ask about the cyber attack, because that is a relatively new phenomenon that a lot of people don't know a lot about. They may get a virus on their computer or something like that, but they really don't understand. In your estimation, how bad could a cyber attack be? I have heard some people talk about a digital Pearl Harbor. What is kind of the worst case scenario for a cyber attack, in your estimation?

Mr. WATSON. Well, first of all, it is not as good or as bad as you see in a lot of the press. You can see comments all over the spectrum. The Internet is probably the most resilient and redundant communications means that we have ever developed. It would be very unlikely that it would be disabled because—for many reasons. It is resilient. It is redundant, as I have said. But the bad guys use the Internet like we do, to share information or to spread information or to gather information. So they don't want to take down the infrastructure on which they depend any more than we would want it to come down.

That said, if terrorists had the wherewithal to delay or confuse a 911 response system while they were conducting a physical attack, they could theoretically increase the number of casualties and delay the response to protect those citizens, and that is the one that would worry me.

Senator PRYOR. OK. Do you feel like we are taking steps to avoid that scenario?

Mr. WATSON. We are taking a lot of steps. The sectors are very engaged and we are improving the security responses in everything from control systems, all the way through communications and interdependencies.

One area I think we could work better on is regional interdependency exercises so that every region and every city knew who the stakeholders were in all the sectors and they had exercised through all these options and knew the backup plans they need to put in place.

Senator PRYOR. In your view, is that something that could be coordinated by the Department of Homeland Security?

Mr. WATSON. I believe it is and I think it is in their plan to do that.

Senator PRYOR. OK. Thank you.

Mr. Stephan, let me turn to you. I know it looked like a couple of times you wanted to chime in there and maybe add a little something. Did you want to add anything before I ask you questions?

Colonel STEPHAN. No, sir. I am pretty much in agreement with Mr. Watson's response. He has been a great partner and his leadership has been personally very effective in building a lot of bridges and certainly they are not shy in bringing problems and issues to us through the PCIS and at the individual sector level. That is what the partnership is all about and we continue to solicit that

feedback. Every suggestion that these folks pass up or issue they pass up, I take action on or explain to them why I am not able to do it so at least we have that very positive and direct feedback loop going back and forth.

Senator PRYOR. Good. Let me ask about these sectors that we have talked about here, these 17 sectors. One of the first questions I have is when you try to get information from them, who do you get information from? For example, the food sector is such a broad, wide-ranging sector. Who do you get information from and how do you manage that information?

Colonel STEPHAN. Sir, there are two different levels of information and collection, if you will. One is sector-level information in terms of strategic risk concerns for the sector, general concerns, how each sector does incident management. We work through the Sector Coordinating Council framework, sometimes through the PCIS if it is an issue that crosses multiple sectors. Using that approach, again, that is more for strategic-type information needs.

Then we have another level that is a little bit more challenging because we need individual vulnerability and consequence information that we need to draw in many cases from individual companies or corporations across the 17 sector landscapes. I get information from them, sometimes again using the Sector Coordinating Council framework, but more importantly and probably most importantly, my direct information venue now is my Protective Security Advisor cadre, those 17 folks representing my boots on the ground, my eyes and ears forward in very critical locations across the country that have developed trusted relationships with State and local partners as well as private sector partners down to the individual facility level.

Cracking this nut is tough in terms of risk. We are using a tiered approach and we have identified through our partnership model approximately 2,500 things out of the tens and tens of thousands of things that represent infrastructure nodes across the country, things that we would classify as a tier one or tier two by sector, meaning certain consequence and threat and vulnerability criteria. We work through the Sector Partnership model, through the Coordinating Councils, and with individual facilities to gather information relative to their vulnerabilities and consequences and how a threat vector of a particular nature might affect them. That process was kick-started a couple of years ago to drill down so we could focus on those things that we all considered to be mutually important.

Senator PRYOR. OK. Let me ask a similar question to what I asked Mr. Watson a few moments ago about information going back and forth between the government and the private sector. Again, I know sometimes the government is very reluctant to share classified information. That is understandable and I understand why the private sector is reluctant to share proprietary information or just very sensitive information, whatever it may be. But do you feel like that the government is doing an adequate job in sharing classified information under the right circumstances and do you feel like you are getting enough information from the private sector?

Colonel STEPHAN. Sir, on the classified piece first, we have enabled about 900 private sector leaders across the 17 sectors to get a secret-level security clearance, so they come into our classified world and actually give us advice and recommendations as we are building the intel products that affect their world and help us translate from intel speak into private sector speak, if you will. That is one important piece.

But I think the most important piece is working with the intelligence and law enforcement community, the CIA, the FBI, and others, kind of ingraining within those organizations the need to declassify using the tear-line construct, tearing off sources and methods, normally the facts and figures associated with threat information or maybe at the "for official use only" or at the completely unclassified level.

I have been with the Department since day one. It was a very difficult process 4 years ago to declassify information in real time to get it to the private sector. We can do that now, for example, in this emerging threat scenario with respect to the London and Glasgow events, the JFK events, the events associated with the group that was going to be focused on Fort Dix in New Jersey, very quickly, I mean, within a matter of hours, declassifying information, forming tear-line pieces of it, using our information network to blast it out through the PCIS and the individual Sector Coordinating Councils across the United States to our various private sector partners. That is dealing with government to private sector information exchange.

On the flip side, information that we require of the private sector, the key is trust, trust that we will be able to protect the information that the private sector provides to us that is of a proprietary nature or that is of a very specific vulnerability or consequence nature so that they, in fact, don't actually focus terrorists on them through this process.

Before we published the final Protective Critical Infrastructure Information Rule, I think we had a whopping total of 48 vulnerability submissions from the private sector, about a year and a half ago. Since the publication of the final rule, since now everybody knows what the real deal is and they can study it, they can have their lawyers focus on it, we now are over 5,400 individual vulnerability assessment submissions in the span of the last 18 months. So we continue to climb the chart now in a geometric fashion instead of trickling them in a few dozen or so maybe in a year's time frame. That is very important.

Getting education and awareness through the Sector Coordinating Councils, through the PCIS, down to the companies that this is how your information will be protected is very important, but the true test of time of all of this will be when PCII hits the judicial process for the first time and we have a successful court case that will show the private sector that this will withstand judicial scrutiny and we will get a favorable ruling. Until that happens, there will be a shadow of doubt in the private sector's mind that the court system will allow this information regime that we have put in place to stand.

So again, doing everything we can to work with the folks, help them understand why we need the information, how it will be pro-

tected, final rule out the door, building up that trust through my PSAs and others at the individual jurisdiction or company level, and finally, this will have to go through the court process to make a 100 percent determination.

Senator PRYOR. In the last few days, Secretary Chertoff has been in the news about perhaps increased threat level in the summer months, and the Department of Homeland Security, a couple years ago established this color-coded threat level. Do you incorporate that in what you are doing? In other words, do you look at various infrastructure and say, well, this may be a red, this may be a yellow, this may be a green? Do you make that independent assessment?

Colonel STEPHAN. Sir, we make that assessment, but not independently, in concert with State and local government officials, principally the State Homeland Security Advisory Network, and again, through the Sector Coordinating Councils for each of the sectors. I have a general level of protective measures in place that people will go to depending on where we are in the color scale. That has been coordinated over time over the past 3 years.

We used that set of protocols specifically with the transportation sector, the aviation subsector last August when we went from yellow to orange in the aviation subsector, putting in place mutually agreed-to protocols. Some of those responsibilities lie with the Federal Government through TSA. Lots of them, and most of them, in fact, lie with the airports and the airlines through that network.

Senator PRYOR. So in other words, you feel like you have the flexibility—just say, for example, Secretary Chertoff says we generally are in an orange——

Colonel STEPHAN. Yes, sir.

Senator PRYOR [continuing]. But you look at your sectors and you say, well, these couple of sectors are probably more to red and these others may be more to yellow, but nonetheless, you have the flexibility to——

Colonel STEPHAN. We have the flexibility to go up by color by individual sector or subsector, or if we want to not do that, we can, by virtue of our Executive Notification System, our Information Sharing Network, our Sector Partnership Council framework, bringing the folks together and say, based on Intel, we feel it is prudent that this sector, without raising necessarily to orange or red, take additional steps such as the following, and we push those recommendations out the door. But again, we do that in a collaborative fashion via phone conference or face-to-face meetings sector by sector.

Senator PRYOR. All right. Let me ask one last question for you, Mr. Stephan, if I can, and that is, I think it was both you and Ms. Larence testified that the private sector controls about 85 percent of the critical infrastructure in this country. Who controls the other 15 percent, and are we doing something similar with that 15 percent?

Colonel STEPHAN. I would say probably the lion's share of the remaining 15 percent is under State and local government control. For example, a lot of the water sector, municipal governments own water systems throughout the United States. And then probably less than 1 percent is an asset that is owned and operated and pro-

tected by the Federal Government. So our Federal departments and agencies have the least amount of responsibility by ownership across the board, State and local governments next in line, and finally the big lion's share of all this is through the private sector.

We have a similar arrangement. We have a State, Local, Tribal, Territorial Government Coordinating Council, about 30 individuals that represent Homeland Security advisors, emergency managers, law enforcement, public health officials, food and agriculture officials, regulatory officials at the State and local government level. We use them as a sounding board and as an information sharing network much as we do the Private Sector Coordinating Councils.

And, of course, all the grant programs directed at infrastructure essentially provide money that go to State and local communities in concert with infrastructures that happen to reside within their jurisdictions. For example, my buffer zone program that IP owns, $191 million over the past 4 years, 2,200 to 2,400 individual plans that tie inside defense and outside defense considerations together that unite State and local government, law enforcement with private sector security people to have a web of security that extends beyond the fence line or perimeter of a facility. That is how we need to collaborate together.

Senator PRYOR. OK. Let me ask one other follow-up. When the Department of Homeland Security was founded, the Critical Infrastructure Assurance Office (CIAO), is that what you call it?

Colonel STEPHAN. Yes, sir.

Senator PRYOR. It migrated from Commerce to DHS.

Colonel STEPHAN. Yes, sir.

Senator PRYOR. CIAO has started to try to get an assurance program for each U.S. department, is that right?

Colonel STEPHAN. Sir, the CIAO in its form 4 years ago no longer exists. Those individual entities, five or six of them that came forward into the Department of Homeland Security no longer exist as individual entities. They are now interspersed among the divisions of the Infrastructure Protection Office or the Cyber Security and Communications Office. That early work by the CIAO has been superceded by the 17 Sector-Specific Plans, and a principal component for the Federal departments and agencies is the Government Facilities Sector-Specific Plan, where a lot of that pioneer work by the CIAO has been embedded or integrated.

Senator PRYOR. OK, great. That sort of ties up a loose end for me, because I didn't know how that worked. Thank you.

Ms. Larence, let me ask you a few questions here. I believe in either your testimony or report, you talk about the turnover rate at Homeland Security and its effect on trust, just human nature being what it is, when you have a lot of new people and you haven't had a chance to build those relationships. What do you think we can do or should do, or how can we help alleviate that problem and build that trust? What do we need to do there?

Ms. LARENCE. I don't know if I can address the turnover rate, but in terms of trust, this is an issue that we continue to identify in our reports over probably about the last 4 years. Some of the sectors did report to us that it has been improving, that they have been building effective relationships with their counterparts within DHS and that has helped the sectors progress. I think not only the

turnover, but the lack of expertise about the sectors and how their businesses operate is also another gap that might be something that DHS could address, perhaps through additional arrangements with contractors or intergovernmental personnel arrangements where you could bring folks in to learn about the industries' business.

Senator PRYOR. Let me ask, in your testimony a little bit earlier, you talked about plans to plan, and as I understand, what you were saying is that sometimes these efforts really result in plans to make a plan, but they never really get to the plan. Is that what you mean by that?

Ms. LARENCE. The NIPP process is really about describing the process that sectors will use to get to the end point of identifying their critical assets and making sure they are protected, and so the NIPP was really just requiring the sectors to identify how they would go through that process.

Senator PRYOR. And, by the way, do you think that has been successful so far?

Ms. LARENCE. All of the sectors have met those baseline criteria.

Senator PRYOR. OK.

Ms. LARENCE. But if you look at the plans, some of the sectors that are more mature, for example, banking and finance, if you read their plans, they will indicate that they have identified a lot of their critical assets. They have risk and vulnerability assessments in place. They have been regulated. Their examiners have been doing risk assessments on a wide part of the industry.

And so you can tell some sectors have gone through more of those steps, whereas if you look at, for example, public health or food and agriculture, they are really just getting their sectors organized and they are still at the very front end of that process where they are trying to make sure they have the right people at the table, quite frankly, and then begin to determine what criteria they would use to figure out what their most critical assets are across a widely diverse base. I think food and agriculture points out that they have millions of farmers, two million farmers, and 150 meat packing processing plants that they have to bring to the table. Health care has 13 million health care professionals, 6,000 hospitals and a number of other facilities and labs. So just trying to get their arms around what their sector looks like and how to manage that diversity is a real challenge for them.

Senator PRYOR. You apparently testified before the House Homeland Security Committee, 3 weeks ago, something like that?

Ms. LARENCE. We did a member briefing yesterday, sir, and before Appropriations several months ago.

Senator PRYOR. OK. Let me ask about the plan-to-plan idea and how some sectors are further ahead than others. Overall, what is your overall assessment of how we are doing in this effort? I mean, are we halfway there? Are we a quarter of the way there? Are we almost there? What is your general assessment of how we are doing?

Ms. LARENCE. Well, in terms of actually designing and implementing the plans, we asked the chairs of each of the Private Sector Councils for their opinions, their own opinions of where they were, and I would say that most of them characterize themselves

pretty much at, on a scale of one to five, at about a three. I think they feel that their large, most critical facilities or assets, were at least doing risk assessments or had them under control. They still have a lot of work to do to really get that sector-wide perspective.

A couple of sectors felt that they were at a one or a two, that they had pretty much moved through the process and really had identified their assets and had conducted risk assessments and had protection measures in place, and a couple of the other sectors, as I mentioned, the public health and food and agriculture, some of those that are newer, recognized that they were probably more at stages three, four, or five, where they had a ways to go.

That doesn't mean that those sectors' assets, however, are not protected, because as we mentioned, individual owners and operators, because of simply business operations or continuity of operations, or maybe the regulatory requirements for security, have taken some steps to make sure their assets are protected. So we don't want to mislead that the assets in those sectors are, in fact, unprotected. It is just trying to figure out as a whole, across the sector, where are we.

Senator PRYOR. Given your analysis and your review of the situation as it currently stands, if most of the sectors right now would give themselves maybe a three on a scale of five, if we were to have this same hearing a year from now, would they come in at fours and fives or would they still be at about a three?

Ms. LARENCE. I think we are trying to get them to ones or twos, but I think a lot of them, if you look at their sector plans and the milestones that they had set out for them, have a pretty ambitious plan, I think, over the next year or two to move through that model. So I think we would see a lot more progress.

Senator PRYOR. OK. Good. Did anybody want to follow up on anything the other witnesses have said?

Colonel STEPHAN. Sir, just one. I hardly ever am in disagreement with my colleagues from GAO, because they do a wonderful job. They have a significant amount of challenges. I would just question the phrase, "plan to plan." I think that where we are is that every sector now has a baseline plan, and as you see from that list, these sectors—the only thing they share in common is that they are all different, all very unique. Most of them are huge, with the exception probably of the nuclear energy sector. There is a fairly tight, very tight, closely knit circle of friends there with a very small number of facilities that is under a security-regulated environment.

I would say that all of these plans represent plans that have deliverables, milestones, and timelines that are concrete that set a baseline. These plans will be reviewed and updated on an annual basis, as required. But all of them have tangible things that they have signed up to with metrics to measure their performance embedded inside the plans that they have agreed to as a public-private sector partnership, and I would characterize them in that context as opposed to plans to plan, because I feel pretty strongly, I am not in this business to plan anymore. I am in this business to implement. We have a year and a half left in this Administration, and for my mission responsibility, no more planning except for, for example, in the case of avian flu, where we do have a few more

steps to make at the sector level to put the final loops into that and close them.

These things are a baseline. Some sectors are higher than others in terms of where they are in progress. That is by virtue of the fact of who they are, what their risk landscape looks like, how many actors are in there, how dispersed are they, so on and so forth. So I would just add that to my testimony.

Senator PRYOR. Ms. Larence, did you have any comment on that?

Ms. LARENCE. Two, if I may, sir. Just one following up on cyber. I promised my colleague in our IT team to plug, as a separate effort, that they went through all the sector plans specifically looking to what extent they identified cyber issues, as Mr. Watson was referring to, and they will be releasing that report probably later next week.

Similarly to our findings, they determined that to some extent it varied, the extent to which sectors considered their cyber assets in their sector plans. For example, as he mentioned, control systems. It is important that sectors think about where their critical cyber assets are and integrate those into their plans. So I think we still have some work to do with some of the sectors on that.

The other thing I would just mention under information sharing, something to watch that is developing at the State level are State information or intelligence fusion centers, and each State has been creating those now to fulfill, I think, a gap that they found within their State jurisdictions to have information that their governors and that their State and local folks could use. We have been doing some work looking at those fusion centers and they are now beginning to look, some of them, at how they can bring the private sector into those fusion centers, as well, which would give them some more direct access to intelligence and information.

Senator PRYOR. Right. We have been talking about that on the Subcommittee, as well, so that is good.

Does anybody else want to comment?

Mr. WATSON. I might have one more point, just to reemphasize the need to look at the regional interdependency issue. Terrorists and Mother Nature don't attack sectors, they attack individual areas, and this has been a very valuable exercise to develop sector-wide principles and guidelines for security measures. It has been valuable for us. In the IT sector, the first thing we had to do was define the sector. Who are the members and what are the key functions? How do we look at the dependencies of those functions, and what are the cross-sector interdependencies? So that has been very valuable for us.

But we need to always keep in the forefront of our minds that it is a regional emphasis. We need to build from there and look at the multiple sectors that are uniquely connected in each region of the country.

Senator PRYOR. Good. Well, listen, I want to thank the witnesses again. We will keep the record open for 15 days. All of our colleagues on the Ad Hoc Subcommittee may submit questions in writing. If they do submit any questions, I would like you all to respond to those as quickly as you could.

I want to thank you all and let you know that your written statement will be made part of the record, and if you have other docu-

ments or studies that you want to be part of the record, we will be glad to include those, as well.

So thank you again for being here and thank you for your testimony.

[Whereupon, at 3:17 p.m., the Subcommittee was adjourned.]

APPENDIX

Statement for the Record

Alfonso Martinez-Fonts, Jr.

Assistant Secretary, Private Sector Office
Office of Policy
Office of the Secretary
Department of Homeland Security

Before the

Committee on Homeland Security and Government Affairs

Subcommittee on State, Local and Private Sector Preparedness and Integration

United States Senate

"Private Sector Preparedness Part I – Defining the Problem and Proposing Solutions"

June 21, 2007

2:00 P.M, Dirksen Senate Office Building, SD-342

Introduction

Chairman Pryor and Members of the Committee.

I am Al Martinez-Fonts Jr, Assistant Secretary for the Private Sector within the Office of Policy at the Department of Homeland Security, and I am pleased to respond to the Committee's request for information about public-private cooperation in emergency preparedness and response.

In order to adequately inform the Committee and respond to its request we are providing information about the Private Sector Office itself, which is a unique creation in the Executive Branch; various characteristics, requirements and experience with public private partnerships; specific information about Private Sector Office activities in support of public-private cooperation in emergency preparedness, response and recovery; and examples of activities by several other components of the Department, excluding in part, FEMA, which is represented here today and the Office of Infrastructure Protection, which will be able to address this subject to the Committee in further detail in the near future.

Part I – The Private Sector Office

The U.S. Department of Homeland Security's Private Sector Office (PSO) is an outgrowth of the position of Special Assistant to the Secretary, created in Title I, Section 102(f) of the Homeland Security Act. The Special Assistant was given seven enumerated tasks designed to promote cooperation between the Department and the private sector. The Private Sector Office was created as a result of requests made to Congress by major business associations who recognized that more cooperation between the Department and the private sector was very desirable to enhance our nation's homeland security efforts. The Intelligence Reform and Terrorism Prevention Act of 2004 added three more tasks to the original seven in the Homeland Security Act.

In condensed form, the statutory mandates for PSO are to:

- Create and foster strategic communications with the private sector;
- Advise the Secretary on the impact of Department's policies, regulations, processes and actions on the private sector;
- Interface with Federal agencies with homeland security missions to assess their impact on the private sector;
- Create and manage Private Sector Advisory Councils;
- Work with Federal labs, research and development centers, academia to develop innovative approaches and technology;
- Promote public-private partnerships to provide collaboration and mutual support;
- Develop and promote private sector best practices to secure critical infrastructure;
- Coordinate industry efforts regarding DHS functions to identify private sector resources that could be effective in supplementing government efforts to prevent or respond to a terrorist attack or natural disaster; and

- Consult with various DHS components and the Department of Commerce on matters of concern to the private sector.

The Private Sector Office has evolved to a staff of fourteen Federal personnel, with additional contract staff support. The Private Sector Office is now part of the Policy Office where it is better able to satisfy its statutory mandate.

The Private Sector Office has two divisions: the Business Liaison Division and the Economic Analysis Division. The Business Liaison Division works directly with hundreds of individual businesses, trade associations, nonprofits, and other professional and non-governmental organizations, ranging from the U.S. Chamber of Commerce and the Business Executives for National Security (BENS) to the American Red Cross. The Business Liaisons also work with the Department's components, as well as with other Federal agencies, including the Small Business Administration, the U.S. Department of Labor, U.S. Department of Commerce and the U.S. Department of Health and Human Services.

The roles and examples of activities of the Business Liaison Division include:

Obtaining information from the private sector to advise senior leadership and the policy development process by:

- Conducting preparedness efforts, infrastructure protection outreach and education;
- Facilitating immigration issues/TWP outreach work;
- Encouraging Work Place Enforcement sessions and discussion;
- Facilitating Safety Act listening sessions with industry;
- Providing situational awareness to current and emerging issues (i.e., effects of regulation on the chemical industry, travel industry impacts of WHTI, effects of immigration legislation on U.S. employers);
- Contributing to numerous Department initiatives (i.e., non-immigrant visas/Rice Chertoff Initiative, etc.); and
- Pandemic preparedness seminars with HHS/CDC.

Creating and fostering strategic communications with private sector by:

- Creating and sustaining relationships with U.S. Chamber of Commerce, Business Roundtable (BRT), National Association of Manufactures (NAM), Business Executives for National Security (BENS), National Federation of Independent Business (NFIB), American Society for Industrial Security (ASIS), as well as many Critical Infrastructure/Key Resource (CI/KR) and non-CI/KR associations;
- Facilitating discussions and relationships with major corporate leaders (i.e. Wal-Mart, Home Depot, General Electric, financial services sector leaders, etc.);
- Conducting topic-focused roundtables for the Department to receive insight and awareness from private sector leaders (large and small businesses, associations/NGOs); and

- Participating in the process of delivering government information (threat response, mitigation, etc.) to the private sector.

Promoting DHS policies to private sector by:

- Delivering speeches and presentations to various groups and constituencies communicating Homeland Security policies, actions and initiatives; and
- Working with DHS leadership, Public Affairs and other DHS components to shape and target communications and provide strategic engagement of private sector leaders and key constituencies.

Supporting outreach to the private sector by DHS components by:

- Aiding rollouts and operations (e.g., US VISIT, National Response Plan (NRP), National Infrastructure Protection Plan (NIPP), etc.);
- Facilitating private sector member/association involvement in national and regional preparedness exercises (e.g. TOPOFF 4)
- Participating in incident communications and operations during an event of national significance. For example, coordinates staff forward to the Joint Field Office, ESF 15 (External Relations) operations; and private sector assistance to FEMA (i.e. establishing networks/relationships, large donations);
- Obtaining private sector inputs to DHS Strategic Plan, NRP, NIPP and similar products; and
- Contributing to improved Border crossing operations (i.e., 25% Challenge in Detroit, Mariposa Port of Entry, Nogales, AZ).

Facilitating and encouraging public private partnerships by:

- Working with the *Ready* Campaign, specifically *Ready Business*, to encourage owners and operators of small to medium sized businesses to create a business emergency plan, to talk to their employees and to take steps to protect their assets; and
- Coordinating with State and local business coalitions such as Pacific North West Economic Region (PNWER), Great Lakes Partnership (Chicago); Security Network (San Diego); Pittsburgh Regional Coalition for Homeland Security, Washington Board of Trade, ChicagoFIRST, State and regional BENS affiliates, Bankers and Brokers Roundtable, Hispanic Chamber of Commerce.

Encouraging the commitment of private sector resources into homeland security activities by:

- Promoting business continuity and supply chain security and resilience; and
- Encouraging coordination/integration of cyber and physical security.

The Private Sector Economic Analysis Division works with the Policy Office, other DHS components, other Government agencies, and external organizations to obtain

information and analyze issues. More specifically, its roles and actions include the following:

Providing economic analyses of current or proposed Homeland Security actions, rules and regulations to offer component agencies and senior leadership with additional insight and perspective by:

- Assessing the consequences of cyber attacks;
- Evaluating Pandemic Influenza efforts;
- Conducting air traveler customer surveys;
- Reviewing U.S. VISIT survey/analysis;
- Assisting U.S. Citizenship and Immigration Service (USCIS) in developing proof of concept analysis for their Transformation Project; and
- Coauthoring *Risk Assessment of Collecting Antidumping Duty and Analysis of CBP Bonding Policy* for CBP.

Reviewing regulations, including providing help to regulating agencies by:

- Assisting the Transportation Security Administration (TSA) in the completion of various rulemakings and their subsequent rollouts (i.e., REAL ID, APIS, ADIZ, trucking hazardous materials);
- Providing comments and assisting USCIS on completing the proposed rule on Religious Worker Visa Program; and
- Working with USCIS, ICE and the Chief Procurement Officer on estimating the costs of various components of the IMAGE (ICE Mutual Agreement between Government and Employers) programs.

Part II – Public Private Partnerships

Public-Private Partnerships (PPPs) directly or indirectly help address preparedness and consequence management issues. This section identifies the types of participants, some of the roles and purposes of such PPPs, the requirements for successful PPPs, the risks that they may not be successful, major variabilities among PPPs, their result, and many diverse examples of PPPs in addition to the following abbreviated examples.

The PPP is quite different from the traditional government relationship which treats the private sector as more of a supplier or customer. "Partnership" requires a different mental attitude for all participants. It implies "give and take", not a "take it or leave it" philosophy. Both the government and the private sector partners have constraints, (e.g. legislative, contractual, financial, or staffing), which limit their ability to agree on actions. However, the expectation is that neither the public nor the private sector will "win every argument" and, instead, will work collaboratively to achieve mutually beneficial goals.

Stakeholders of Public Private Partnerships

There are many possible participants in PPPs. The public sector participants could be agencies from one or more levels of government: Federal, State or local. In most cases,

the government participants do not involve the senior agency official. The private sector participants in the PPP can include individual businesses, trade associations, civic organizations, nonprofits and non-governmental organizations like American Red Cross.

The Purpose of Public Private Partnerships
Public Private Partnerships have many potential roles and purposes. Some are focused on preventing terrorism while others combine protection and preparedness actions, to include both acts of terrorism and natural disasters. Still others may focus only on natural disasters but their results can be transferable in either case. PPP's may have one or more of the following purposes, some of which can overlap:

- For Federal, State or local governments to provide and receive information related to acts of terrorism and natural disasters;
- For private sector organizations to learn, understand, and influence prospective decisions by governments regarding prevention, protection and preparedness relative to acts of terrorism and natural disasters;
- For governments responding to a disaster, to encourage cooperation with private sector, who may be able to provide donations of goods or services, restore utilities or essential services to pre-disaster status, or work to reduce the impact of a disaster;
- For governments to obtain economic information useful in aiding in its recovery, evaluating disasters and reducing potential impact of mitigation decisions;
- For private sector organizations to mobilize with government to address disaster related issues which are critical to the private sector; and
- To solve security and expedited movement of people and goods across our borders.

Characteristics of Public Private Partnerships
Most PPPs are not created under a specific legislative mandate. There are several characteristics of PPPs that could be characterized as "requirements" in order for a PPP to be successful. Some are addressed in written documents, many are not. They include:

- A charter with agreed scope for work and collaboration; success requires clear mutual goals defined before PPP begins;
- Agreed commitments to and expectations of the new PPP, including staffing and budget required of each party;
- A designated leader from the government and one from the private sector, who can address any issues which may arise;

- PPPs can be initiated by the private sector or the government, although most are initiated by the government. Many times the government, initially, persuades one or more key private sector partners to join the effort. They, in turn, help recruit other private sector members. In order to persuade the private sector to participate, there needs to be a "business case", or "value proposition;"

- Compatibility between the PPP purposes and the mission and goals of government agency and private sector partners is essential; and

- Individuals in both the government and the private sector who are "champions" or "promoters" for the partnership are very important, particularly where the "business case" is not very strong.

Challenges to Successful Implementation of Public Private Partnerships
Public-Private Partnerships are vulnerable to risks and challenges which can lead to their termination or change of course. Some risks can be addressed; others cannot. The risks may include:

- Concern by the private sector regarding potential liabilities regarding sharing information with governments and for voluntary actions taken to assist in recovery from disasters. Many businesses would like to collaborate; however, there are many liability issues. These concerns, whether perceived or real, inevitably may inhibit the private sector from participating in a true partnership.

- Ability of businesses and organizations to assist. Many who have the capacity and resources to make a significant impact in emergency preparedness, response, and recovery often are suppliers of goods and services. In this position, government may view this as a conflict of interest.

- Priorities of the government or private sector partners can change which may lead to a reduction in commitments and/or expectations on either side;

- Loss of "champion" or "promoter;"

- Proliferation of PPPs which involve same private sector or government organizations may lead to confusion, conflict or "partnership exhaustion";

- Mishandling or inappropriate sharing of information by either government or private parties leads to loss of trust and credibility;

- Favor of individual firms by Government if PPP excludes their competitors;

- Understanding level of participation. Unless the "business case" for participation is understood at the beginning of the PPP, it may not survive long.

Variability Among Public Private Partnerships
There is no single model of public private partnership that supports the prevention, protection against or preparedness for natural disasters or terrorist actions. Some of the variations between PPPs include:

- Whether a particular partnership should be ad hoc for a specific disaster or issue or continuing;

- Level of involvement of local, State, or national level or a combination of one or more levels; and

- Number of participants and budget, which can range from few and no allocated budget to hundreds and annual budgets measured in thousands of dollars.

Results and Impacts from Public Private Partnerships
Over 85% of the critical infrastructure and key resources in the United States are owned or operated by the private sector. Federal, State and local governments in the United States are neither authorized by law nor have the funds to provide comprehensive protection to each critical infrastructure asset. Thus unless the private sector takes actions to prepare for, respond to, and recover from an act of terrorism or natural disaster, the country will be poorly prepared to deal with these possibilities.

While the private sector can do so on their own, greater impact occurs when they collaborate through Public Private Partnerships. Many Public Private Partnerships have been created in the past five years and few have been terminated, a sure sign of progress which has helped to further enhance the information sharing, preparedness, and protective actions necessary to help ensure the security of the Nation.

Almost every review of the United States' efforts to prepare to prevent, protect against, respond to, and recover from terrorist or natural disasters urges the continuation and increase in public private partnerships to achieve that end. Although there are no available statistics on numbers or results of PPPs, the fact that there is still willingness and desire by both the private sector and governments to create PPS is a strong indication that the results and impacts of PPPs have been very positive.

Successes of Public-Private Partnerships
PPPs directly or indirectly help address preparedness/consequence management issues and help protect critical infrastructure.

Some examples of PPPs:

- The Office of Infrastructure Protection coordinates and facilitates Sector Coordinating Councils of private sector organizations representing each of the 17 Critical Infrastructure/Key Resource Sectors. These councils work with government agencies through the Critical Infrastructure Partnership Advisory Council to share information and develop means of preventing, protecting against and preparing for terrorist disasters.

  In addition, the Office of Infrastructure Protection coordinates the National Infrastructure Advisory Council (NIAC) which provides the President through the Secretary of Homeland Security with advice on the security of the critical infrastructure sectors and their information systems. The NIAC is composed of a maximum of 30 members, appointed by the President from private industry, academia, and State and local government.

- The Office of Intelligence and Analysis officials work with State and local authorities at fusion centers across the country to facilitate the two-way flow of timely, accurate, and actionable information on all types of hazards. In Washington State, for example, representatives from the private sector sit side by side with government.

  Fusion centers provide critical sources of unique law enforcement and threat information; facilitate sharing information across jurisdictions and function and provide a conduit between men and women on the ground protecting their local communities and State and Federal agencies. The Department will have tailored multi-disciplinary teams of intelligence and operational professionals in fusion centers nationwide by the end of fiscal year 2008.
- The Homeland Security Advisory Council (HSAC) provides advice and recommendations to the Secretary on matters related to homeland security. The HSAC is comprised of leaders from State and local government, first responder communities, the private sector, and academia. In 2007, the HSAC Private Sector Work Group created "The Future of Terrorism Task Force Report" and the "Homeland Security Culture Report."

- The Science and Technology Directorate facilitated the establishment of the Homeland Security Science and Technology Advisory Committee. This was established in 2004 to serve as a source of independent, scientific and technical planning advice to the Under Secretary for Science and Technology as mandated by the Homeland Security Act of 2002.

- The National Communications System has had an active partnership with the telecommunications industry since its inception in 1962. NCS coordinates the National Security Telecommunications Advisory Committee of 30 industry executives who advises national leadership on exercise of telecommunications functions and responsibilities and the coordination of the planning for and provision of national security and emergency preparedness communications

for the Federal government under all circumstances, including crisis or emergency, attack and recovery and reconstitution.

The National Security Information Exchange (NSIE) process was established as a forum in which government and industry could share information in a trusted and confidential environment to reduce the vulnerability of the Nation's telecommunications systems to electronic intrusion. The NSIE process continues to function today, demonstrating that industry and government will share sensitive security information if they find value in doing so.

- The Transportation Security Administration regularly works with key air transport organizations. In the event of a disaster, TSA works with these organizations to assist in the disaster response efforts. For example, during Hurricane Katrina, TSA, through its ongoing relationship with the Air Transport Association (ATA) facilitated air transportation from ATA member airlines to over 20,000 disaster victims.

- The Office of Cyber Security and Communications (CS&C), is working in partnership with the Office of Infrastructure Protection, Sector-Specific Agencies, and public- and private-sector security partners, is committed to preventing, protecting against, responding to, and recovering from cyber attacks and their consequences. CS&C's strategic goals include preparing for and deterring catastrophic incidents by achieving a collaborative risk management and deterrence capability with a mature information sharing partnership between government and the private sector. This strategic goal also encompasses tactical efforts to secure and protect the Nation's cyber and communications infrastructures from attacks and disasters by identifying threats, vulnerabilities, and consequences.

  A number of initiatives are currently under way to identify vulnerabilities to the Nation's critical infrastructure, assess their potential impact, and determine appropriate mitigation strategies and techniques. CS&C supports the management of risk to the information technology and communications sectors' critical functions and infrastructures that support homeland, economic, and national security; it works to reduce the likelihood of success and severity of impact of a cyber attack against critical infrastructure control systems; detects and analyze cyber attacks; and facilitates the identification of systemic risks across the Nation's CI/KR sectors.

- Customs and Border Protection, in coordination with FEMA, is requested to assist during significant incidents for Law Enforcement and Public Safety (Emergency Support Function 13), Search and Rescue (Emergency Support Function 9) and Transportation (Emergency Support Function 1). Due to the various missions CBP currently employs each day at our borders, these

functions assist in incident response and management. CBP's role and direction are dictated by FEMA to their mission during an incident.

The Private Sector Office staff is assigned a portfolio which over many of our largest components such as Customs and Border Protection, Immigration and Customs Enforcement, the Transportation Security Administration and the U.S. Coast Guard. The Private Sector Office often acts as a catalyst with Department components to cultivate and foster public-private partnerships.

Part III – Private Sector Office Actions Specific to Emergency Preparedness, Response and Recovery

The Private Sector Office works with Department components to assist in the establishment of relationships, integration and partnership building with the private sector. Taking FEMA as an example, we are:

- Dedicating PSO staff to assist FEMA in their efforts to integrate the private sector in their mission critical priorities;

- Spearheading the development of private sector expertise into FEMA operations. PSO and FEMA are working with loaned executives from the private sector to provide advice and best practices especially in the areas of logistics, operations and communications;

- Advocating and advising FEMA on the importance of private sector coordination as apart of FEMA's newly established National Advisory Council;

- Implementing Hurricane Katrina lessons learned in regards to donation management. During Hurricane Katrina, the Private Sector Office created the National Emergency Resource Registry (NERR) to register the flood of unsolicited products and services. Since then, the NERR framework was retooled to create the Debris Contractor Registry. This is an electronic database developed to assist State and local governments in identifying and contacting debris removal contractor resources. The information provided and maintained by contractors and their representatives.

  To replace NERR and address the need for donation management during a crisis, FEMA reached out to AIDMATRIX, a nonprofit organization who, through a grant from FEMA, has created a virtual superhighway for all levels of government, private sector, and nonprofits to connect and share unsolicited offers of products, services and volunteers both for crisis management and everyday mission support.

  Supporting the development and outreach objectives of the Pandemic Planning Guide for Critical Infrastructure and Key Resources. This guide was

created in partnership with HHS/CDC based on the principles of the national standard for business continuity, the NFPA 1600;

- Advocating and supporting private sector coordination in national and regional exercises such as the upcoming TOPOFF 4 and the Department of Defense-sponsored ARDENT SENTRY;

- Actively encouraging State and local coordination with the private sector. Just last month we worked with the City of Charlotte and the Charlotte Chamber and the U.S. Chamber of Commerce in the design and development of the Charlotte Regional Business Preparedness Summit;

  This summit provided the business community with Federal resources, a forum to engage Charlotte's Office of Emergency Management and its local first responder community, a forum to engage Federal, State and local public health officials regarding Pandemic Flu, a showcase to highlight best practices in Charlotte's business community on the importance of business continuity of both small and large businesses and finally, a first hand opportunity to learn the fundamentals of business continuity as outlined by the NFPA 1600.

  This event was a pilot initiative with our office and the U.S. Chamber to increase engagement of business owners and operators on the importance of business continuity planning, emergency response coordination and pandemic flu preparedness. In partnership with the Ready Campaign, we are working to develop a toolkit for State and local officials to be able to replicate these types of business preparedness summits across the country, especially during National Preparedness Month;

- Supporting the active use and outreach of programs like *Ready Business* whose content is based on the Preparedness and Business Continuity Standard NFPA 1600 as developed by the National Fire Protection Association and endorsed by the American National Standards Institute, the 9/11 Commission and the U.S. Department of Homeland Security, *Ready Business* resources and tools encourage owners and operators of small to medium sized businesses to create a business emergency plan, talk to their employees and take steps to protect their assets;

- Providing support and advisement for September's National Preparedness Month. In 2006, the Private Sector Office assisted in recruiting hundreds of businesses to become National Preparedness Month Coalition partners to promote workplace and community preparedness;

In addition, PSO also reaches out across to Federal Interagency. For example, PSO is working with the DHS Office of Infrastructure Protection to coordinate with the Department of Energy on several initiatives such as encouraging the owners and operators of gasoline stations to wire and install generators to operate fuel pumps in case

of a power outage. In past collaborations with DoE, the Department worked to sponsor exercises that include the electrical and oil and natural gas industries, in exercise design and tests of detection, response and recovery from terrorist attacks and natural disasters in order to identify lessons learned and needed changes to protocols and invited industry participation in a lessons learned forum following the 2005 hurricane season to identify best practices and needed changes to preparedness, response and recovery;

In partnership with SafeAmerica and the U.S. Chamber of Commerce, PSO participated in a series of Pandemic Flu Preparedness Events across the country. PSO reached out to the DHS Chief Medical Officer, the DHS Office of Infrastructure Protection and to the U.S. Department of Health and Human Services to promote joint pandemic outreach initiatives.

Summary

Public Private Partnerships have existed in the United States for many years. They often have very diverse membership involving one or more levels of government and can also involve varying numbers of private sector organizations.

One essential characteristic of a successful Public Private Partnership is that it must provide clear benefits to all parties, including a shared and valued outcome. These benefits constitute the "value proposition" of the Partnership and define the motivations and contributions that members bring to it.

There are very many types of Public Private Partnerships. The more successful have a scope and purpose that results in continuing benefits to the public and private participants and also have "champions" in both the public and private sectors. Mishandling of shared information between the public and private participants, changing goals of government or private sector partners, loss of "champions", and potential liability for sharing information are among the main risks that can cause premature termination of Public Private Partnerships.

The results and impacts of Public Private Partnerships for preparedness, prevention and protection have been very positive and increasing during the past five years both from pre-existing partnerships and from newly created ones.

PPP's are not "disguised charity" by the private sector. Good PPPs serve common public/private sector interests, and private partners must be chosen carefully based on their business interests and resources. PPPs are not a means to shift the public burden away from government. However, a "partnership" in its truest state, is where both partners contribute their core skills and services as a joint effort. This collaboration creates an environment which builds trust, communication and cooperation. These results only enhance our nation's ability to better prepare for, respond to, recover from and mitigate against an act of terrorism or a natural disaster.

Statement for the Record

Marko Bourne

Director of Policy and Program Analysis
Federal Emergency Management Agency
Department of Homeland Security

Before the

Committee on Homeland Security and Government Affairs

Subcommittee on State, Local and Private Sector Preparedness and Integration

United States Senate

"Private Sector Preparedness Part I – Defining the Problem and Proposing Solutions"

June 21, 2007

2:00 P.M, Dirksen Senate Office Building, SD-342

Introduction

Chairman Pryor and Members of the Committee.

I am Marko Bourne, Director of Policy and Program Analysis and Evaluation at the Department of Homeland Security's Federal Emergency Management Agency.

You have heard Administrator Paulison discuss his vision for a "new FEMA." The new FEMA will develop operational core competencies by implementing a business approach designed to lead the Nation's domestic preparedness, protection, mitigation, response and recovery missions by forging stronger public-private partnerships, implementing new business and management practices, incorporating lessons learned, and strengthening our dedicated and professional workforce. These steps will enhance our agency's capacity to--

- Lead the Nation to better prepare against the risk of all-hazards, including terrorism;
- Marshal an effective national response and recovery effort;
- Reduce the vulnerabilities of lives and property;
- Speed the recovery of communities and individual disaster victims; and,
- Instill public confidence when it is needed most – in the hours and days following a disaster.

The new FEMA is becoming more valued than before across all jurisdictions – Federal, State, local and tribal, and private sector, as a proactive, engaged, agile and responsive leader and partner in preparedness and emergency management.

We at FEMA are working diligently to build this new organization, while leveraging the solid foundation of expertise and accomplishment brought to FEMA by core elements of the former DHS Preparedness Directorate that, since April 1st of this year, are now a part of FEMA. These past and ongoing preparedness activities are being integrated with the actions and initiatives that FEMA has been taking for the past 18 months to improve operational efficiency, build mutually beneficial partnerships, learn best practices, and gain valuable insight on how we can and should operate in the future.

In particular, FEMA is focused on improving its relationships with the private sector by focusing on key areas such as preparedness partnerships, internal organizational assessments, enhanced supply stream management and logistics, contracting, catastrophic planning, strong community coalition building, and industry fairs and outreach.

As the committee considers private sector preparedness efforts and challenges, at FEMA we are working closely with the DHS Private Sector Office (PSO), the Office of Infrastructure Protection (OIP), the Office of Public Affairs and others to strengthen the outreach to a critical partner in our response to any emergency. In order to achieve a greater level of private sector preparedness, many businesses have updated their business continuity plans based on their lessons learned from Hurricanes Katrina, Wilma, and Rita and are working with emergency management officials at local, state and federal levels to

get more involved in planning for disasters that may affect the cities and regions in which they operate. FEMA is also engaging the private sector to assist us in our efforts to build a stronger emergency management system. Through the National Incident Management System (NIMS) and the National Response Plan (NRP) revision process, FEMA and OIP worked with industry representatives to include language in NIMS that integrates the private sector as a full partner in incident management.

Preparedness Partnerships

Of course, FEMA does not and can not do it alone. We rely on all of our partners across the emergency management spectrum. Increasingly, we are leveraging the resources and expertise of our partners in the private and non-profit sectors – even above and beyond the important role they have always played in the past.

This increased reliance comes about because the new FEMA is developing innovative ways to be more forward leaning and quicker to respond appropriately to disasters or emergencies. One way we are doing this is through a dramatic increase in pre-scripted Mission Assignments and pre-negotiated contracts to provide necessary resources.

We are also doing it through the vast portfolio of grant programs FEMA now manages which supports implementation of the Interim National Preparedness Goal. The Goal outlines an all-hazards vision that cuts across the four mission areas of preparedness: to prevent, protect, respond and recover from major events, including terrorist attacks and catastrophic natural disasters. The Goal is truly national in its scope, in that its successful implementation requires engagement across Federal, State, local, and tribal levels, as well as the private sector and individual citizens.

Also, DHS' grant programs allow a tremendous amount of flexibility for State and local jurisdictions to include private sector entities in planning efforts. Allowable activities include the development of public/private sector partnership emergency response, assessment and resource sharing plans, development or enhancement of plans to engage with the private sector/non-governmental entities working to meet human service response and recovery needs of victims and the development or enhancement of continuity of operations and continuity of government plans.

Although many of FEMA's grant programs award funds to state or local governments to implement projects that support their State or Urban Area Homeland Security Strategies, ongoing coordination with private sector partners - particularly on key issues related to critical infrastructure protection where the private sector owns 85% of the assets - is absolutely necessary. The private sector plays a vital role in the planning process that supports the implementation of preparedness grants in the field. Recognizing this vital role, FEMA has engaged organizations such as Business Executives for National Security (BENS), the U.S. Chamber of Commerce, and the Council for Excellence in Government to further the dialogue on preparedness.

One exception is the Urban Areas Security Initiative (UASI) Nonprofit Security Grant Program (NSGP) for which nonprofit organizations in the 46 designated UASI areas are

eligible. This grant program, announced this past April, will provide over $24 million to eligible 501(c)(3) organizations who are deemed high-risk of a potential terrorist attack. Through this program, we are working with the private sector to enhance their security.

FEMA's Port Security Grant Program (PSGP) is a second exception. PSGP is open to public and private owners and operators of critical port infrastructure. Overall, PSGP has provided more than $1 billion to public and private entities since its inception in Fiscal Year (FY) 2002. Most of the funding in initial years of this program was awarded to federally-regulated private entities. Over the last 2 years, however, public entities received a higher proportion consistent with the DHS approach to securing critical infrastructure.

The Intercity Bus Security Grant Program (IBSGP), Trucking Security Program (TSP), and the Transit Security Grant Program (TSGP) are also available to the private sector. Similar to PSGP, these programs are focused on our nation's critical transportation infrastructure. In the case of the IBSGP and the TSP, 100% of the awards are made to private entities. IBSGP is targeted exclusively to commercial over-the-road bus entities to enhance the security of intercity bus systems that service Urban Area Security Initiative (UASI) sites. Through the IBSGP, DHS has awarded a total of more than $60.5 million to commercial owners/operators of over-the-road buses providing fixed route services or charter bus services in high risk regions since FY 2003.

Since FY 2003 DHS has provided over $62 million, through TSP, to the American Trucking Association (ATA), supporting operations of the Highway Watch® Program to enhance security and overall preparedness on our nation's highways. Through the Highway Watch® Program, a cooperative agreement with the American Trucking Associations, highway professionals are recruited and trained to identify and report security and safety situations on our Nation's roads. ATA has used these funds to train more than 400,000 commercial truck drivers in highway security domain awareness and to operate a nationwide call center for truckers to report security incidents.

Funding for the TSGP is used to enhance the security of rail transit systems including commuter, light and heavy rail; intra-city bus; inter-city passenger rail (Amtrak); and ferry systems. Additionally, the Intercity Passenger Rail program, part of the TSGP, was created in FY 2005 to provide assistance to Amtrak to improve security to its passengers and to date DHS has awarded approximately $22 million under this program.

Another significant example of public- private partnering is through FEMA's new Training and Education Division, which has a number of courses being developed or delivered that are available for private sector participation. For example, the new online training relating to the National Infrastructure Protection Plan (IS 860) is designed to be used by both government and private sector security partners. More than 3000 individuals have taken this course since it was posted this past year.

The National Exercise Division (NED) works closely with the Department's Private Sector Office and Office of Infrastructure Protection (OIP) to develop a systematic means

to integrate the private sector into national level exercises as well as taking steps to coordinate for future modifications to the Homeland Security Exercise and Evaluation Program that will encourage and guide State and local efforts to construct exercise activities inclusive of the private sector.

Moreover, private sector entities continue to be involved in the Hurricane Preparedness Exercise activities that are sponsored by the NED on an annual basis. Finally, NED, through its Direct Support Exercise Program, works with Major League Baseball, the National Football League, and other activities that involve venues that attract large concentrations of citizens to organize and conduct exercises to ensure preparedness for large scale incidents at these venues.

The U.S. Department of Homeland Security and the Advertising Council launched the *Ready Business* Campaign in September 2004. This extension of Homeland Security's successful *Ready* Campaign, designed to educate and empower Americans to prepare for and respond to emergencies, focuses specifically on business preparedness. *Ready Business* helps owners and managers of small- and medium-sized businesses prepare their employees, operations and assets in the event of an emergency.

Ready Business was developed by Homeland Security and launched in partnership with U.S. Chamber of Commerce, Small Business Administration, Society of Human Resource Management, The Business Roundtable, The 9/11 Public Discourse Project, ASIS International, Business Executives for National Security, International Safety Equipment Association, International Security Management Association, National Association of Manufacturers, National Federation of Independent Businesses, and Occupational Safety and Health Administration.

The goal of *Ready Business* is to raise the business community's awareness of the need for emergency planning and motivate businesses to take action. The campaign encourages business owners and managers to: plan to stay in business; talk to their employees; and protect their investment.

Ready Business also has a Spanish language companion, Listo Negocios, which provides several Ready Business tools and resources translated into Spanish.

The campaign's messages are delivered through: television, radio, print, outdoor and Internet public service advertisements (PSAs) developed and produced by the Advertising Council; brochures; www.ready.gov and www.listo.gov Web sites; toll-free phone lines 1-800-BE-READY and 1-888-SE-LISTO; and partnerships with a wide variety of public and private sector organizations.

In May 2006, the Ready Campaign launched *Ready Business* Mentoring Initiative. This initiative is designed specifically to help owners and managers of small and medium-sized businesses prepare for emergencies. Materials were created to assist business and community leaders in hosting and delivering business preparedness workshops and training sessions. These sessions and the Ready Business Mentoring Guides outline how

businesses can plan to stay in business; talk to employees; and protect assets. Workshop materials were provided through collaboration through USDA Cooperative Extension Service funded Education Disaster Extension Network (EDEN).

To reach businesses and business organizations across the country, the Department reached out to U.S. Department of Commerce, Small Business Administration, U.S. Department of Agriculture and the nation's leading business organizations to distribute the Ready Business Mentoring Guides and access to its resources.

In addition to the Ready Business Mentoring Initiative, the Department also works with the private sector to encourage the adoption of the NFPA 1600 at the local level. For example the Department collaborated with the U.S. Chamber of Commerce on a pilot initiative to create a Regional Business Preparedness Summit in Charlotte, North Carolina. This event brought together local leaders in emergency management, public health and the private sector. Local businesses learned the importance of creating and exercising their business emergency plan, involving their employees, protecting their assets and plugging into their local emergency management network.

FEMA is also integrating the private sector in a myriad of initiatives across the Agency. For example, we are working closely with Homeland Security's Private Sector Office to utilize their concept of relationship and partnership building with the private sector. We have embraced Homeland Security's Private Sector Office staff part of our senior advisors. We are working together on initiatives where we can integrate the private sector into our communications, outreach and operations or by their expertise in such mission critical areas like logistics.

A few highlights of our new approach to the private sector are:

We are taking a proactive approach to leading the way for the private sector to be incorporated into our emergency operations. They will need to be part of a greater public-private partnership 501(c)(3). We are paving that way for this seat to be part of the Joint Field Office, the Regional Response Coordination Center and here in Washington at the National Response Center.

We are incorporating private sector expertise into our operations by creating the FEMA Loaned Business Executive Program. This initiative brings seasoned experts from the private sector into FEMA operations to serve as advisors and collaborate on mission critical programs.

Other initiatives include:

- Private Sector participation in Regional Emergency Communications Coordination Workgroup.
- Memorandum of Understanding (MOU) with the Stadium Owners/Operators.

- Pilot program with Infragard in Denver, Colorado.
- Mutual Aid for businesses.
- Mutual Aid Training for businesses.
- Developing Pilot Website to serve as repository for to post information about the above activities, training opportunities, business continuity, as well as referrals to founding organizations.
- Establishing a Credentialing Work Group to pinpoint issues and begin to develop viable options to address credential concerns.

Internal Organizational Assessments
At the end of last year, Administrator Paulison initiated a series of 17 independent Agency-wide organization assessments as part of his commitment to lead FEMA to become the Nation's preeminent emergency management and preparedness Agency. The completed assessments established a baseline of FEMA's key systems, processes and capabilities in the areas of acquisition and contract management; finance and budget; human resources and disaster workforce; information technology, security, facilities, and logistics. The recommendations were built upon public and private best practices and were documented first in initial reports and then later in January 2007 in the 17 Final Reports. FEMA has moved quickly to implement the recommendations.

Enhanced Supply Stream Management and Logistics
Enhanced supply stream management was evident in FEMA's emergency food supply in 2006. While it was a short-term success, this year we have taken our plan to the next level. Instead of building up our own stockpiles – with the accompanying costs and potential liabilities – we have signed agreements with the Defense Logistics Agency and competitively awarded contracts to other suppliers to be on-call for needed meals and resources. These agreements will improve our response by relying on established, national networks rather than trying to develop our own in the midst of a disaster. Improved logistics is just one of the areas where FEMA is working with partners to make major reforms.

FEMA's new Logistics Management Directorate is enhancing a critical core competency by developing a disciplined, robust, and sophisticated supply and service capability. Logistics Management will transform its capability by increasing involvement with the private sector, including identifying and examining private sector best business practices and processes. To facilitate this involvement, Logistics Management sponsored market research in collaboration with the DHS Private Sector Office and the U.S. Chamber of Commerce. This new logistics organization will be one that is proactive and couples 21st century technology and a professional workforce with strategic public and private partnerships. In pursuit of this enhanced capability, Logistics Management is analyzing its current business operations, its management practices and exploring the use of Third Party Logistics (3PL) providers for its transportation and warehouse management missions.

To further develop and enhance coordination with logistics partners, including the private sector, FEMA will conduct a Demonstration Program with state and local governments to formulate innovative public and private logistical partnerships that will improve readiness and increase response capacity. The Demonstration Program will present an excellent opportunity for FEMA to explore new approaches to logistics management as part of its transformation to a state-of-the-art national disaster logistics capability.

As with many of FEMA's operational offices, Logistics relies heavily on the private sector to provide critical operational support through competitively awarded contracts. Logistics has contracts with private sector for:

- National Commercial Bus Transportation Contract – Third party services for bus transportation. This contract provides over 1,000 coach buses for evacuation purposes. While evacuation is not a federal responsibility, we do have a responsibility to ensure that we are prepared to help states in crisis by providing this key asset.

- Base Camp support – In the aftermath of a disaster, FEMA is often required to house its own response personnel, as well as personnel from State and local governments, other federal agencies, and volunteers. Under this contract, our private sector partners will be responsible to house all authorized camp occupants with tents or modular units, equip tents and other facilities with air conditioning and heating, and leveled plywood floors, as well as provide bedding, meal services, kitchen, dining hall, limited recreation facilities, operations center, medical unit, refrigerated trucks, shower units, hand wash units, potable (drinking) water, water purification and manifold distribution systems, toilets, on-site manifold distribution of black and grey water and associated on-site sanitation systems, complete laundry service, industrial generators, and light towers.

Contracting

The first priority of FEMA during the initial phase of a major disaster is and has always been to provide relief to victims in the most efficient and effective way possible in order to save lives and property. FEMA's goal is to use competitive strategies while also providing local and socioeconomic businesses a competitive advantage whenever possible. FEMA had some pre-negotiated contracts in place before Hurricane Katrina; however, the extreme circumstances of storms like Hurricanes Katrina and Rita demonstrated that these few contingency contracts could not sufficiently meet mission requirements. As a result, many non-competitive contracts were needed in order to effectively and efficiently save lives and property.

Due to the magnitude and length of recovery time of Hurricanes Katrina and Rita, FEMA has recognized the need for more robust, well-planned contingency contracts and a thorough understanding of the qualifications and capabilities of the private sector in areas related to the Agency's mission. Since Katrina and Rita, FEMA has worked to

aggressively award pre-negotiated competitive contracts, and these are in place and ready for the 2007 hurricane season. Contract agreements are in place covering all aspects of FEMA disaster management including logistics, mitigation, individual assistance, recovery, management, and integration center support.

By having advance contracts or similar agreements in place, FEMA as well as State and local first responders are more organized and efficient. Additionally, coordination is made easier among the federal, state and local governments, as each entity is aware of the goods and services for which FEMA has already contracted in the event of disaster. This increased coordination makes for a more effective and efficient response.

FEMA is particularly committed to working and partnering in advance with industry partners from the small and disadvantaged business community as well as local companies within disaster areas. The Agency is accomplishing its goal of benefiting these businesses through numerous initiatives, including:

- Participating in outreach forums to meet with the Small Business Community;
- Conducting personal meetings with interested vendors/contractors to present company capabilities and performance;
- Developing goals and acquisition strategies which are increasingly structured for maximizing the number of awards to small businesses;
- Networking with representatives of the U.S. Small Business Administration and local small business development centers;
- Participating in local, state and national conferences, seminars, and exhibits to gain access to current small business issues and interface with business and industry; and,
- Creating a voluntary, debris removal contractor registry to enable small and local firms to notify FEMA, and interested state and local governments, of their capability to support disaster response and recovery requirements as needs arise.

Catastrophic Planning

FEMA's Disaster Operations Directorate has collaborated closely with the DHS Private Sector Office (PSO) and Office of Infrastructure Protection (OIP) to ensure continued visibility with the private sector of Federal, State, local, tribal, and critical infrastructure coordination and activities related to responding to catastrophic disasters and FEMA's Catastrophic Disaster Planning Initiative. As part of the U.S. Chamber of Commerce's Business Civic Leadership Center and its Homeland Security Division's Annual Workshop, the Chamber sponsored a session on June 7-8, 2007, in conjunction with the PSO to discuss response to and recovery from a New Madrid Seismic Zone Earthquake. One of the primary topics of discussion was how the private sector develops partnerships in planning to meet the challenge of responding to such an event and integrate planning between the public and private sector. A comprehensive report detailing the results of the workshop, recommendations, and how the business community can partner with Federal, State, local, and tribal governments and critical infrastructure owners will be prepared and used as we move forward with the Catastrophic Disaster Planning Initiative not only for the New Madrid Seismic Zone, but also for the Florida (Category 5 Hurricane

impacting Southern Florida), and California initiatives. The eight New Madrid Seismic Zone States (Alabama, Arkansas, Illinois, Indiana, Kentucky, Mississippi, Missouri, and Tennessee) will begin conducting Catastrophic Disaster Response and Recovery Planning Workshops this summer. The Chamber workshop served as a catalyst to begin the private sector participation in these initiatives.

The State of Florida has already initiated a series of workshops to address response and recovery planning for a Catastrophic Category 5 Hurricane impacting South Florida and planning for catastrophic earthquakes in California is now in the initial phase.

Important components needed to make the Catastrophic Disaster Planning Initiative a success include involving the private sector and business community to the maximum extent possible; establishing solid partnerships between the public and private sectors and non-governmental agencies; and highlighting the critical role the private sector can play in providing supplemental resources and assistance in catastrophic disaster events.

Integrating Critical Infrastructure Protection as a key component of Catastrophic Panning and Incident Management

FEMA, in collaboration with OIP, has done extensive work with the private sector in the development of processes to integrate the protection of critical infrastructure and key resources as a key component of incident management, which is critical to catastrophic planning. As a result of the lessons learned from Hurricane Katrina, FEMA and OIP worked closely together with other Federal departments and agencies and private sector partners to develop processes for addressing disaster-related requests from private sector Critical Infrastructure/ Key Resources (CI/KR) owners and operators. The processes also utilize the partnership model established in the National Infrastructure Protection Plan to enhance incident related information-sharing and decision making relating to CI/KR. The engagement of this public-private partnership as a component of incident management is important because the vast majority of the infrastructure in our country is owned and operated by the private sector. Having an established mechanism to foster coordination strengthens our ability to respond to the full spectrum of 21st century threats.

Strong Community Coalition Building

More than ever, we at FEMA are building stronger and more vibrant community coalitions by giving the private sector a more prevalent role in emergency response through FEMA's Citizen Corps Program. Citizen Corps' primary mission is to bring community and government leaders together in an all-hazards emergency preparedness, planning, mitigation, response, and recovery framework. The Citizen Corps nationwide network includes more than 2,200 Citizen Corps Councils located all 56 states and territories. Councils are encouraged to include business representation and to work with businesses to integrate business resources with community preparedness and response plans. An important priority for Councils at all levels is to educate and inform Americans in all sectors—including the private sector—about steps they can take to be prepared. The Citizen Corps program works closely with the Department of Homeland Security's Ready Campaign, making Ready Business and other Ready materials widely available. Furthermore, Citizen Corps encourages its Councils to work with local emergency

management and to incorporate work continuity plans and planning in specific community context.

Citizen Corps' Partner Programs also collaborate with businesses. National Partner Programs include more than 2,600 Community Emergency Response Teams (CERT) and hundreds of Fire Corps, Medical Reserve Corps, Neighborhood Watch, and Volunteers in Police Service programs around the country. Many CERTs already include the business community in their training and exercises. For example, the San Diego County CERT has trained local utility and telecomm employees as part of their partnerships, and many CERTs have adapted the curriculum to business needs, providing Business Emergency Response Training for employees.

In addition, Citizen Corps Councils are encouraged to build strategic partnerships with local governments and businesses to use some existing grant funds for their coordinated training activities and exercises. Many local Citizen Corps Councils have also developed partnerships with major retailers to provide discounts and education on supplies to help families prepare for disasters. For example, Utah Citizen Corps volunteers worked with all 47 Wal-Mart stores statewide to promote preparedness during "preparedness weekends." Wal-Mart has also donated $10,000 to support the program, paid for the Citizen Corps booth at the 11-day Utah State Fair and donated printed material on emergency preparedness. Clear Channel also provided free graphics for the Utah Citizen Corps billboards placed throughout the State, focusing on the "Be Ready Utah" campaign. During the holidays, they worked together on a media campaign encouraging Utah residents to remember preparedness items on their shopping lists.

Industry Fairs and Outreach

In an effort to create stronger partnerships with the private sector, and to better learn from their best practices and what they can do to help FEMA and the nation during a disaster, FEMA has held two important industry fairs to meet with key partners.

On April 16-17, 2007, FEMA hosted a Manufactured Housing Workshop with several key manufacturers dealing with all phases of the housing program, including those from the travel trailer and mobile home industry. The first day was focused on the new Uniform Federal Accessibility Standards (UFAS) specifications FEMA adopted for travel trailers and mobile homes to be used in future disasters. On the second day, FEMA and the participants discussed creative acquisition solutions and possible new inventory management concepts to be used by the housing program. Participants learned about FEMA's Joint Housing Solutions Group and a new assessment tool, which provides a structured process to evaluate options and explore alternatives to manufactured homes. This new software evaluates housing options using several factors including cost, timeliness, community acceptance, range of use, and livability, and creates an opportunity to match needs to available housing units. Industry representatives showed great interest in contributing data and suggestions as well as reviewing evaluation results. FEMA is committed to working with our partners in the manufactured housing industry. Continued collaboration is vital to the success of FEMA's housing program.

On May 16, 2007, FEMA hosted a Passenger Airline Industry meeting to solicit from the airline industry how the federal government might best make use of commercial passenger aircraft to support the transport of evacuees from large populated areas rendered uninhabitable by either an anticipated or actual major event to safe and secure locations. The event provided a forum for dialogue among FEMA, its Federal partners, and industry on efficient and cost-effective ways to provide air evacuation support. The discussion covered two important issues: evacuation flight operations and pre-positioning of aircraft. There were approximately 70 participants, including air industry trade groups and associations who represented national and regional commercial air carriers; major commercial airlines; charter passenger air carriers; aircraft brokers and intermediaries; airport authorities; and commercial airline industry regulators.

This meeting had three primary objectives aimed at addressing the air transport of evacuees: 1) to enhance FEMA's ability to conduct mass air evacuations; 2) to explore all available options in the commercial passenger airline industry; and 3) to establish air transport capacities and performance requirements. There was a general consensus that industry could play a role in supporting flight operations to evacuate citizens prior to and immediately following a large-scale disaster. They have the capacity, capabilities, and expertise. FEMA's new burgeoning relationship with the air industry will continue in hopes of finding viable solutions to executing a large scale potential evacuation within the United States.

The private sector is also engaging both FEMA and state emergency management to provide liaison to state emergency operations centers, joint field offices and we are working with the Chamber, BENS and BRT about developing a private sector association liaison in the National Response Coordination Center. We also have scheduled a meeting with those three groups the week of June 26, to discuss several additional partnership efforts to build on our individual discussions.

Some of our planned efforts include bringing private sector "executives on loan" to FEMA to assist us in our planning, logistics and management reform efforts. This will allow us to improve our business practices, develop 21st century logistics programs and provide a better link to the private sector during emergencies.

Conclusion – A Call for Continued Public-Private Communication and Partnership

There will certainly be a continuing role for the private sector in the future. We at FEMA need to insure we are adapting to new conditions, adopting innovative and more effective business practices and addressing ever changing needs. To do this, we want to hear from and work with all audiences with a stake and a responsibility in preparedness and disaster response.

FEMA is reaching out to our partners in other Federal, tribal, State, and local agencies and building better relationships with the non-profit and private sectors. As you are aware, the worst time to build relationships is during a disaster.

In FEMA's opinion, the private sector should continue and build upon efforts in several key areas:

1. Developing strong business continuity plans for all of their locations and critical data centers.
2. Develop employee support plans for when their employees' office locations are damaged or if their employees have lost their homes to disaster. A key element of recovery is getting people back to work as quickly as possible
3. Engage in prudent risk management practices and have strong health and safety programs.
4. Work closely with their local emergency managers, first responders and elected officials to be involved in disaster planning and to build protocols to assist with recovery efforts, before a disaster strikes.
5. Through business associations continue to work with state emergency management and FEMA to support preparedness planning, disaster response, donations management, and recovery efforts.
6. Engage private sector partners through planning, training, and exercise activities, the resulting relationships and shared vision can only help to strengthen our nation's preparedness.

FEMA appreciates the relationship we are developing with the Chamber, BRT and BENS and believe this ongoing dialog will produce an improved flow of information and support before, during and after an event. It is the work and resources we expend on this planning now, before a disaster that will pay dividends later in a quicker recovery and a more resilient nation. We cannot wait till the disaster occurs to exchange our business cards and the private sector understands that it cannot just show up on game day and expect to play without coming to the practices.

One of the most important lessons learned from the 2005 hurricane season is that in order to ensure a successful, robust, and coordinated response we must work together on all critical fronts, horizontally and vertically, across the full spectrum of emergency management, including government, private sector, non–profit organizations and our citizenry.

Thank you for the opportunity you have afforded us today to speak about the new FEMA. I look forward to addressing your questions.

Statement of
F. Duane Ackerman

Before the

Subcommittee on State, Local, and Private Sector
Preparedness and Integration
of the
Committee on Homeland Security and Governmental Affairs
United States Senate

June 21, 2007

Mr. Chairman, members of the Committee, thank you for the opportunity to testify today on "Getting Down to Business: An Action plan for Public-Private Disaster Response Coordination." I am Duane Ackerman, former Chairman and CEO of BellSouth Corporation. I am also a member of Business Executives for National Security (BENS). BENS is a national, non-partisan organization of business and professional leaders dedicated to the idea that national security is everybody's business. Its members apply their experience and expertise to improving the business of national security. In that spirit and commitment I served as Chairman of the BENS Business Response Task Force, which produced the report I am here to talk about today.

Invited by the senior leadership of both the United States Senate and U.S. House of Representatives to offer advice, in June 2006 BENS formed a Task Force to recommend to the U.S. Government steps to systematically integrate the capabilities of the private sector—principally those of the business community—into a comprehensive national disaster response mechanism.

BENS did so in response not only to the federal government's recognition of a pressing need in the aftermath of Katrina, but also in response to the overwhelming demand of its membership. During the summer and autumn of 2005, my company, BellSouth – and many, many companies across the country – experienced first-hand the reality that the role of business in response to national disasters has not been appropriately established—neither at the local and state nor at the national level.

In preparing this report, the Task Force assiduously mined the wealth of experience of its members and other executives—completing nearly 100 interviews—in developing its findings.

During the late summer and fall of 2006, the report, in draft form, was circulated widely and briefed to federal and congressional agencies and staff,

the White House, senior leaders at the National Governors Association and the Association of State Attorneys General, the US Northern Command, professional associations and to corporate leaders around the country. While the conclusions are those of the Task Force, the report benefits immeasurably from comments and suggestions made by our government and business colleagues.

The report's recommendations fall into three substantive categories: public-private collaboration; surge capacity/supply chain management; and legal & regulatory environment. In addition, the report specifies priorities and sequencing for implementing its recommendations.

Time does not permit us to discuss in detail the breadth of analysis and conclusions in their entirety. With the Chairman's permission, I would ask that the entire report be submitted for the record.

Today, I want to discuss with you what our Task Force revealed about the private sector and its role in response to disasters, both natural and man-made. Our aim was to build up what US Comptroller General David M. Walker, during his March 2006 testimony before your full committee, called the "total force"—by which he meant the coordinated assets of federal, state and local authorities, the military, non-profit organizations, *and the private sector*. The goal I set before the Task Force was to ensure that in large-scale disasters, the full breadth and depth of private-sector capabilities and resources are available when local, state and federal officials are all at the scene together.

The 100 surveys we conducted reaffirmed several truths that Task Force members recognized from their own experiences. First, disasters happen regularly and businesses routinely plan for un-forecast events. Second, businesses in the "strike zone" have extensive experience collaborating with public-sector first responders. Third, after securing their own operations, businesses invariably move to help ensure the continuity of the community.

Continuity of community is a key concept for officials charged with preparing the federal emergency response to consider. In a disaster, which always begins in a locality, support from the private sector is typically automatic, not only because businesses are citizens of their own communities, but also because without continuity of community no business can be done. In thinking about the Task Force's aims, it soon became clear that a key goal was determining how to scale effective local responses up to a true national response capability.

Our surveys revealed nine main themes that must be satisfied to re-establish continuity of community at the local level and, I believe, are equally applicable to creating an efficient national response. I will run through them very briefly and then focus on a single recommendation that we, the Task Force, believe would be worthy of your endorsement and support.

Business Preparedness: The first theme to emerge from the surveys was that companies' experience in preparing for crisis is extensive and applicable to government preparations.

The vast majority of large businesses, and many smaller ones, have a continuity plan in place. Nearly all companies stressed the importance of training their employees and crisis management leaders.

Example: Major retailers know to stock up on extra supplies during hurricane season and position them just outside the hurricane zone in order to be able to deliver them immediately after a storm passes. Government needs to leverage that private-sector capacity and plan for its use.

Relationships: The second theme is that relationships must be established in advance of a crisis. Companies must pursue pre-crisis relationships for their own continuity plans by developing lines of communication among employees and senior executives; with neighbors, suppliers and even competitors; and with government authorities at all levels.

Authority: The third theme is that there is a lack of clarity about who is in charge once governmental authority escalates from the local to the state and federal levels.

Example: One organization told an interviewer that while FEMA was at one door to help, the Customs and Immigration Service was at the other, trying to remove those whose visas were invalidated because the organization was closed for business (even though closure was due to the very same hurricane that its fellow DHS agency was addressing via recovery efforts).

Communications: The fourth theme is that operational and accurate communications are vital. Crisis wreaks havoc with technology to be sure, but the problem transcends technology. During Katrina, even when a company could feed into a government source, it was frequently reported that the information available was often confusing and inconsistent, particularly when multiple government authorities were on hand.

Example: If the land lines aren't working—which they are not if the power is down—you only have cell phones. But they have restrictions as well: one is the power to the towers, and two, their backup batteries only had a short useful life....So in any business that is spread out,... you're basically out of business. For one company, this season all of the senior executives have three separate cell phones on different systems, hoping that at least one of the systems will be up and operating.

Logistics: The fifth theme is that business needs improved methods to deliver goods and services to the government or directly to needy communities during a crisis. Interviewees discussed at length government's inability to accept and distribute goods and services in an efficient manner

following Katrina. Everything from food and clothing to medical care came in, but with a woefully inadequate logistics system, ice melted, donated clothing piled up and rotted, and medical personnel were turned away.

Examples: One company had 600,000 tarps available to cover damaged roofs, but the federal government was unable to draw on the supply chain to secure and distribute them. Another company offered to donate three mobile communications units, only to be told that their offer was refused and countered with a request to buy ten of the same. We were told by one interviewee that a senior manager of a large transportation association spent a full day trying—and failing—to locate a single authoritative point of contact within FEMA to coordinate bus deployments. Numerous examples were cited of the government's inability to accept private-sector donations, often because of lack of pre-defined procedure or mechanism for doing so.

Business response: The sixth theme is that like government authorities, some companies also play a role similar to that of first responders, and thus need to be given emergency responder status. Disasters often destroy many key components of a community's critical infrastructure, and business continuity for companies in those industries (such as energy and telecommunications) is an essential component of the community's immediate recovery. Therefore, these corporate first-responders (identified as such by the authorities and prior to a crisis) need to be given priority status with regard to credentialing and access to facilities, affected areas, and information.

Example: Because the private sector plays such an essential role in rebuilding the community, it is important that government agencies generally refrain from commandeering essential goods from corporate first responders. Fuel and power were frequently cited as the most important resources needed early in a crisis. Without those inputs, business cannot proceed and many continuity plans fall apart. One company reported twenty-five pieces of heavy equipment completely under water and damaged. New equipment was ordered but as it was being brought in (to New Orleans for work on a priority federal project), it was commandeered. The company had to send a local sheriff to escort the equipment. Further, fuel from Baton Rouge for the same equipment got commandeered at the checkpoint as well.

FEMA: The seventh theme is that FEMA representatives were replaced far too often, thus resulting in FEMA policies being inconsistently applied and the establishment of working relationships with FEMA on the local level becoming nearly impossible. Also, the mechanisms for establishing two-way communications with FEMA officials on the ground were unreliable from the start and quickly overwhelmed. We trust that recent changes at FEMA have rectified these shortcomings.

The Good Samaritan: The eighth theme is that the vast majority of companies—like the vast majority of citizens—will strive to "do the right

thing" during crises. One can discern from their behavior that business cultures that are not risk-averse on a daily basis will not be risk-averse in a crisis. The challenge is how to transfer this cultural insight from the private sector to government bureaucracies.

Legal and Regulatory Barriers: The ninth theme is that regardless of industry, size, or location, companies found significant regulatory barriers that hindered their ability to execute their own continuity plans, to assist within their communities, assist other communities, and work in concert with government recovery efforts.

Attention to these themes, as I said at the outset, is key to preparing an effective, efficient response at the local, state, regional or national level.

With these challenges in mind let me return to the principal goal of our Task Force efforts: to ensure that the efficient application of private-sector capabilities and resources is preserved as the disaster escalates through local, state, regional and, eventually, federal jurisdiction and action.

Our key recommendation is this: The American private sector must be systematically integrated into the nation's response to major disasters, natural and man-made alike. The Task Force believes that building public-private collaborative partnerships, starting at the local, state or regional level, is one of the most important steps that can be taken now to prepare the nation for future contingencies.

Local, state or regional public-private partnerships are vital to filling gaps in homeland security and disaster response that neither government nor business can manage alone. These partnerships mobilize private-sector cooperation—including the supply of material assets, volunteers, information and expertise—that strengthens our nation's capability to prevent, prepare for, and respond to catastrophic events.

Government and business know intuitively that they need to work together during crisis, but how to do that doesn't come without effort on both sides. Business-government collaborations require a level of trust and agility that is easiest to build at the local, state and regional levels, and they are possible at all levels.

The failure so far to properly integrate the private sector into the government disaster response apparatus, while serious and pervasive, can be remedied. To do so requires a new dedication to effective public-private partnership and, we believe, a new approach: simultaneous, integrated action from *both* the very top of our federal government structure *and* from the state and local levels upward.

The framework we propose is simple and straightforward: Emergency Operation Centers (EOCs), which already exist at all levels of government to

plan for, train and implement emergency responses to disaster, should include a presence for the private sector beyond that which exists today. The private sector, in turn, must maintain parallel Business Operation Centers (BOCs) that can plug-in to government operations and "scale up" with them in a *parallel* and *coordinated* manner as government adapts to deal with disasters from small to large.

Recognizing that it is not possible for all businesses to participate at the "table" at once, the Task Force recommends that BOC membership be generally rotating and structured in three tiers:
1) Critical infrastructure owners and operators as permanent members;
2) Other sectors or companies deemed critical to restoring the continuity of community, represented on an "as available" or voluntary basis. (These seats could be rotating or permanent, based on the number of such businesses or the nature of the functions they provide to the community. Regional or national companies who cannot participate at each local level can be brought into the response as it escalates to the regional or national level); and,
3) Entities representing business at large within the community (Chambers of Commerce, professional or trade organizations, or civic clubs, e.g., Rotary), as rotating participants that can reach back to their business membership for help or information sharing.

The BOC concept creates an operational capability that integrates private-sector resources into emergency response plans. This operational capability is missing from the National Response Plan as currently constructed, and we are hopeful that this capability will be recognized and encouraged in the current revision of the NRP. A Business Operations Center, connected structurally to its corresponding EOC, will greatly enhance disaster-response capability by providing a vehicle to include the private sector in planning, training, exercising and most important, in an actual event.

As simple and logical as this proposition sounds, real business-government disaster response integration is still in its infancy. This integration needs to mature across the country, and fast, if we as a nation are to seriously prepare for the next major calamity. It is my hope, and the sincere recommendation of the BENS Task Force, that you will acknowledge, encourage and support the building and exercising of enduring public-private collaborative partnerships that integrate the private sector into our nation's response infrastructure. In turn, the private sector must have a reliable government partner. Viable partnerships will reflect balanced participation among private, local, state, regional and federal actors in all phases of operations: planning, training, exercising and executing. If this structural reform is adopted, it will greatly facilitate all of the other recommendations in the report of the BENS Business Response Task Force.

Thank you.

Statement of
The Honorable John Breaux

Before the

Subcommittee on State, Local, and Private Sector
Preparedness and Integration
of the
Committee on Homeland Security and Governmental Affairs
United States Senate

June 21, 2007

Mr. Chairman, members of the Committee, thank you for the opportunity to provide testimony today. I am John Breaux, Senior Counsel at Patton Boggs LLP. Last summer, I accepted the invitation of Duane Ackerman to serve alongside The Honorable Newt Gingrich as Co-Chair of the BENS Business Response Task Force. I would like to ask that my full testimony be submitted for the record, as well as the Task Force's report, "Getting Down To Business: An Action Plan for Public-Private Disaster Response Coordination."

Our report, issued in January of this year, focused on institutionalizing an effective and sustainable role for business in disaster preparation and response in partnership with all levels of government. To that end, as you have heard, it offered recommendations in three substantive areas:

1. Public-private collaboration, to plan, train, exercise, implement and evaluate joint actions required to facilitate effective communication, decision-making and execution;

2. Surge capacity for private-sector goods and services, and the capabilities resident in private-sector supply chains, to manage the delivery of goods and services (including pro bono and contracted) to and within disaster areas; and

3. The legal and regulatory environment, which can help or dramatically hinder efficient delivery of private-sector support during a disaster. It's also an important issue after the disaster in terms of economic continuity and recovery in the affected locales.

I would like to focus on this last area—the legal & regulatory environment—because it is in this category that I believe your subcommittee can be most effective in spurring improvement in our nation's disaster-response capabilities. I will conclude with some observations on how we might re-define existing resources to meet the recommendations in our report.

At Duane Ackerman's suggestion, in addition to the chair and co-chairs, the Task Force was comprised of 10 senior business leaders and over 20 expert advisors, divided into three scoping groups; each group was charged with developing recommendations in one of the three focus areas. I served as the senior advisor to the legal and regulatory group, and we set out to deliberate these questions:

- How should government improve Good Samaritan laws to better facilitate the participation of the businesses and business employees that volunteer to help?
- How should legislation, regulation and policy be better aligned at the federal, state and local levels to encourage private-sector preparedness and better mobilize the private sector in a catastrophic event?
- Is revision of the Stafford Act desirable?

After assimilating the results of the Task Force surveys, each scoping group developed recommendations for the *near term* designed to optimize business participation in disaster response. We also developed recommendations for the systematic *longer-term* integration of the private sector into the National Response Plan and its execution in a disaster.

Briefly, here are the findings of the group that I advised:

Business requires a predictable legal regime to operate efficiently in an emergency situation, whether that business is engaged in charitable or profit-motivated activities. The current legal and regulatory environment is neither predictable nor efficient.

Action by the Congress and the Executive Branch is essential for putting into place a legal and regulatory environment in which the private sector can become a full partner in the national response to disaster. We can and must ensure that federal, state and local emergency planners include the private sector in the preparations, testing, training, and execution of their responsibilities. We also must rethink the not-inconsequential issue of the legal allocation of risk through the civil justice system, notably in disaster-related areas of tort law, as well as through regulation.

Based on these findings, the Task Force makes the following recommendations to you, the Congress. Consider:

- Enacting a nationwide body of "disaster law";
- Modifying the Stafford Act to include the private sector; and

- Holding further hearings to determine which Task Force recommendations can be implemented under existing law and which will require new legislation or regulatory action.

Let me amplify the first two points in the belief that doing so will encourage you to hold additional hearings on the full set of recommendations.

NATIONAL DISASTER LAW. Major disasters are a national issue, and uniformity of law across states is essential to the efficient leveraging of the nation's business assets in dealing with them. During the Katrina response, many out-of-state businesses that tried to help had little or no familiarity with the laws of Louisiana or Mississippi, which hurt their efforts and hurt the people of both states. While we must respect the purposes and value of federalism, we should explore nevertheless whether we need a body of federal disaster law to preempt the heterogeneous patchwork of state law in this particular and narrow context.

Two basic principles should guide us in thinking about such a body of law:

- Things should get easier, not harder, and better, not worse, during a major disaster or incident of national significance.

- Individuals and businesses acting in good faith should be able to confidently provide assistance based on a predictable set of rules and responsibilities governing their conduct.

Following the hurricanes of 2005, a great number of laws and regulations necessarily were waived, suspended or modified— two cases in point are certain HIPAA (Health Insurance Portability and Accountability Act) privacy provisions and transportation regulations that inhibited the flow of goods or services to disaster sites. This body of waiver authority should be kept "on the shelf" for consideration in future disasters. In fact, the Task Force went so far in recommending that this issue should be considered in a preventative sense by having federal agencies at the ready to modify other likely provisions in line with the DHS National Planning Scenarios List. Either way, to be effective when invoked, government must communicate with the private sector in advance of and during the crisis so that the predictability standard is met.

REVISE THE STAFFORD ACT. As you know, the Robert T. Stafford Disaster Relief and Emergency Assistance Act is a federal law designed to bring an orderly and systematic means of federal natural-disaster assistance to state and local governments in carrying out their responsibilities to aid citizens. The Stafford Act is a 1988 amended version of the Disaster Relief Act of 1974. The amended act created the system in place today by which a Presidential Disaster Declaration of an Emergency triggers financial and physical assistance through FEMA. The Act gives FEMA the responsibility for coordinating government-wide relief efforts and includes the contributions of 28 federal agencies and non-governmental organizations, such as the

American Red Cross. In October 2000, Congress amended the law with passage of the Disaster Mitigation Act of 2000 (Public Law 106-390), which permitted contributions of federal resources to private nonprofit entities under certain conditions.

The SAFE Port Act of 2006 (P.L. 109-347, Sect. 607) extends the Stafford Act to include the private sector, but only to the extent that it precludes the head of a Federal agency from denying or impeding essential service providers[1] access to the disaster site or impeding them from performing restoration or repair services.

As we saw in Katrina, though, this is not enough. For example, without utilities, banks in the disaster zone—even though they had cash to dispense—could not reopen because they did not have adequate security and local and federal officers would not provide the security requested because the banks were commercial, not public, entities. In light of these and other lapses, several recent congressional actions have proposed changing the Stafford Act yet again, but none of these efforts have been successful. The Task Force believes that Congress should extend coverage of the Act beyond state and local government to include the private sector, with particular attention to enabling the federal government to provide security or protection for private sector personnel and assets operating in a disaster zone. Authorities should be automatic upon presidential declaration of a national disaster, but protections offered should be specific and limited to situations where it is impractical or impossible for the private sector to provide for on its own security.

While remedies to the private sector's full participation in the nation's disaster-response capabilities are urgent, such remedies should not be taken hastily. Adequate consideration and deliberation before deciding to legislate is in order: once in place, law is hard to undo. The Task Force, therefore, urges Congress to review carefully the body of existing law pertaining to disaster response and the agencies of government responsible for carrying out that law. The initial focus of its investigation should be to determine which of the recommendations of this Task Force can be implemented under existing statute, and which require new legislation.

I want to emphasize that the Task Force saw a vital distinction between a need to ensure a predictable legal and regulatory regime, and any alterations to the allocation of risk; it focused exclusively on the former. We recognized that allocation of risk implicates significant, and often contentious, policy issues, and there is no need to address such issues in this context. In contrast, simply ensuring that existing legal standards are clear, stable and

[1] Essential Service Providers include entities that provide telecommunications, electrical power, natural gas, water and sewer services or any other essential services as determined by the President. They include municipal, nonprofit and private, for profit, entities in the act of responding to an emergency or major disaster.

predictable will dramatically increase the ability of the private sector to effectively engage in time of disaster.

Let me conclude with a commentary on financial resources. What I've discussed can be accomplished by you, the Congress, and by the executive branch with little or no additional cost. Our principle Task Force recommendation remains that the American private sector must be systematically integrated into the nation's response to disasters, natural and man-made alike. Building public-private collaborative partnerships, starting at the state level, is one of the most important steps that can be taken now to prepare the nation for future contingencies. The primary recommended vehicle is the already existing network of state Emergency Operations Centers (EOCs).

Most states and major cities already have EOCs. In a few, the broader private sector (that is, not just public utilities) is becoming more integrated through a complementary model that the Task Force calls the Business Operations Center (BOC).[2] As the model scales up to the regional or federal level, sources of funding need to be identified to create and sustain the integration of Emergency Operations Centers with Business Operations Centers. The major investment is talent and time, and the Task Force believes that the private sector itself is willing to commit those resources if it is given its seat at the table.

The Task Force believes that to ensure that the BOC concept takes root nationwide, Congress should direct DHS to develop guidelines and funding for states and urban areas to build BOCs. Currently, grant programs are geared largely to funding one-off exercises and Public-Private communications systems and data interchanges. To address the BOC and cooperation issues, however, such sustained funding through the FEMA grant program should be tied to the requirement that states and urban areas are developing, training and exercising this business-government collaboration. By doing so, the federal government will be taking a tangible step to share this public-private collaborative ethos. It will also be acknowledging the simple fact that businesses will and do get called upon in crisis, and thus, when our government authorities are planning ahead for such, businesses should be an integral part of that preparation.

To be certain, this work is not entirely on your shoulders. For our part, the Task Force has embarked on a number of follow-up initiatives through BENS and its members:

---

[2] Participation in the BOC should represent critical infrastructure and other industries/companies vital to community viability and continuity in crisis situations. Connected structurally to its corresponding EOC, a BOC will greatly enhance government's disaster-response capability by providing a vehicle to collaborate with the private sector in planning, preparation, training, exercises and, ultimately, execution. More information can be found starting on pg 16 of the Business Response Task Force Report.

- The development of a Business Emergency Management Assistance Compact ("BEMAC") concept as a companion to the Emergency Management Assistance Compact structure;

- Assistance to DHS in the revision of the National Incident Management System (NIMS) and the National Response Plan (NRP);

- Work with individual state governments to strengthen Good Samaritan laws to encourage and allow for public-private partnerships in crisis situations; and

- The development of an efficient mechanism by which the federal government might manage the disaster-prompted suspensions of applicable regulations.

To close, the Task Force understands that a comprehensive Congressional review of the legal and regulatory environment surrounding emergency response will require time and effort. For that reason, we urge this body to schedule hearings that will start the process of solving some these longer-term issues. At the same time, we recommend that government seize the opportunity to address the report's short-term objectives, in particular the provision or application of federal financial resources that will enable business and government to train and exercise together. Doing so will be a significant and proactive step towards ensuring that an adequate private-sector response is available for the next disaster—and not one that may befall us many years from now.

Thank you.

RICHARD ANDREWS, PH.D
SENIOR ADVISOR, NC4 (THE NATIONAL CENTER FOR CRISIS AND CONTINUITY COORDINATION)

TESTIMONY
BEFORE THE

SENATE HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS SUBCOMMITTEE ON STATE, LOCAL, AND PRIVATE SECTOR PREPAREDNESS AND INTEGRATON

ON

PRIVATE SECTOR PREPAREDNESS PART I – DEFINING THE PROBLEM AND PROPOSING SOLUTIONS.

THE UNITED STATES SENATE

JUNE 21, 2007

Thank you Senator Pryor, Senator Sununu and other members of the subcommittee for the opportunity to testify today and to discuss some of the work underway to establish processes by which the resources of the private sector might be employed during major emergencies. These efforts include a number of initiatives taken at the state level across the nation and in several major urban areas.

My name is Richard Andrews. I am currently Senior Advisor on Homeland Security for the National Center for Crisis and Continuity Coordination (NC4), a privately owned California company that has worked over the past 5 years to promote situational preparedness and awareness as well as partnerships between the public and private sectors. I am a member of the Department of Homeland Security's Advisory Council where I Chair the Council's Senior Advisory Committee on Emergency Services, Law Enforcement, Public Health, and Hospitals. My previous experience includes service as the Director of the California Office of Homeland Security, Homeland Security Advisor to Governor Arnold Schwarzenegger, and Director of the California Governor's Office of Emergency Services from 1991 through 1998.

I was a member of the BENS Business Response Task Force that developed the report Getting Down to Business: An Action-Plan for Public-Private Disaster Response Coordination. I also serve as Chair of the Private Sector Committee of the National Emergency Management Association (NEMA). NEMA represents the state emergency management directors and serves as the executive agent for

the nation's Emergency Management Assistance Compact (EMAC), which is the operational mechanism by which states exchange resources during major emergencies. EMAC was initially developed by the Southern Governor's Association in the aftermath of Hurricane Andrew and now includes all states as legislatively authorized members.

EMAC and BENS

As highlighted in the 2005 EMAC After-Action report, Hurricanes Katrina and Rita created the largest demand in the country's history for nationwide mobilizations of emergency resources. The two hurricanes resulted in over 2,000 mission requests from the impacted states, requiring almost 66,000 personnel being deployed. Reports produced by the Senate and the White House each cited EMAC as one of the notable successes of the tragic 2005 hurricane season.

In addition, these hurricanes led to discussions between the EMAC leadership, the NEMA Private Sector Committee and BENS regarding the feasibility of using the EMAC processes to promote a more effective use of private sector resources as part of the nation's overall emergency response.

The BENS report identified an obvious shortfall of the 2005 hurricane response -- the fact that there was no systematic process by which the resources of the private sector could be utilized. A number of different efforts - especially the on-the-fly establishment of a national resource registry by the Department of Homeland Security's Office of the Private Sector Coordinator- laudably attempted to facilitate and broker the use of private sector resources. While there were some successes, there was a great deal of frustration within both the public and private sectors. Both sectors recognized the need for greater collaboration, but the absence of a commonly understood process to match needs with available resources -whether donated or contracted - proved to be a major obstacle.

Among the recommendations in the BENS report was the call for building a Business Emergency Management Assistance Compact (BEMAC). The concept is fairly straight forward. By expanding the EMAC program it would be possible to knit together a fabric of state-based Business Operations Centers to create a scalable, flexible and robust "network of networks." Private sector representatives trained in the processes and procedures of a state's operations center would work alongside emergency management leaders to coordinate government and private-sector resources.

Earlier this year, with the endorsement of the NEMA Board of Directors and the EMAC Executive Committee, the NEMA Private Sector Committee initiated an

effort to explore whether the BEMAC concept could be implemented. BENS supported this effort by assigning staff resources to the initiative and my company, NC4, endorsed my chairing the effort.

NC4 has worked in cooperation with the BENS Business Force efforts and other organizations – the Contingency Planning Exchange, the Financial Services Information Sharing and Analysis Center, the American Society of Industrial Security to name a few – to enhance the information exchange and situational awareness for our private and public-sector clients. In addition, with my experience as Director of Emergency Services for the State of California during the 1990s and more recently as the state's Homeland Security Advisor, I believed I had a grounding in the many challenges involved in any effort to enhance public and private sectors interactions.

Working with BENS we formed a Task Force that includes the operational and policy leadership of EMAC as well as representatives from key sectors including retail, pharmaceuticals, medical supply distribution, communications, technology and large-scale logistics. Since February, through a series of conference calls and meetings, we have explored the opportunities, impediments and options for formalizing the processes by which private sector resources might be more efficiently utilized.

One of the Task Force's basic premises was that we wanted to build on, not supplant or unnecessarily complicate the many evolving initiatives across the nation to bring the private sector into the nation's emergency response and recovery network. Our focus has been on the interstate use of private sector resources; in other words, like EMAC, what are the options for linking the deployment of private sector resources from a providing state in support of an impacted state in a manner analogous to the EMAC structure?

Public Sector Best Practices and Barriers to Entry

In order to establish a baseline of understanding of existing efforts at the state and local level to involve the private sector more effectively into the nation's emergency response and recovery networks, the NEMA staff conducted a survey of all states. We designed the survey to both identify current initiatives and best practices as well as real or perceived barriers, especially legal and regulatory, that might inhibit private sector resources from being deployed under the EMAC structure.

The survey clearly revealed that a number of very promising, on-going initiatives are underway across the nation in which states and local governments are

reaching out to the private sector to assist in a formal way in emergency response and recovery efforts. A few notable examples stand out.

The Florida Office of Emergency Management has formally established Emergency Support Function (ESF) 18, "Business, Industry and Economic Stabilization" designed to function during both the emergency response and recovery phases. During the immediate response, ESF 18, together with the State Logistics Section works, with the Florida Retail Association through twice daily conference calls to address strategic supply chain issues, projected and post-event impacts on commercial businesses, and restoration of commercial services. Florida also provides, with state funds, Small Business Emergency Bridge Loans and the establishes Small Business Assistance Centers involving multiple agencies to work with impacted businesses on a variety of recovery issues including regulatory challenges and coordination with federal programs.

Massachusetts also established, in advance of the 2004 Democratic Convention and in cooperation with BENS, a similar "ESF 18" partnership with the private sector that included a resource inventory; the state's emergency management organization continues to expand this initiative.

Texas, following Hurricane Rita, has developed an extensive Private Sector Operations Group consisting of 28 companies to support immediate Mass Care, Fuel, Special Needs, Power, Aviation, and Fuel challenges. These sectors will work alongside the state's emergency management officials to rapidly identify shortfalls in public sector capacity that can be most effectively met by private sector resources.

Utah has organized its Private Sector Homeland Security Coordinating Council as a vehicle to discuss issues of critical infrastructure identification, essential services and key personnel. The state is working on a formal "emergency access" procedure to enable key private sector personnel access to restricted areas. The state is organizing sector-specific coordinating councils that will focus on resource management and is working with local Chambers of Commerce as well as other trade associations to structure a network for communications, resource management, and emergency operations assignments.

New Jersey began working with BENS shortly after September 11, 2001 to develop the New Jersey Business Force. Similar BENS partnerships are operating, in varying stages of evolution, in Georgia, Kansas City, Iowa and the Los Angeles and San Francisco areas. These initiatives include the development of private sector resource inventories that might be available to support state operations, participation by the private sector in New Jersey in TOPOFF 3, other state exercises, and testing the use of private sector facilities and personnel

should mass distribution from the nation's Strategic National Stockpile be required.

North Carolina has formally included private medical personnel and resources as part of the state's emergency response network; these resources were deployed during Hurricane Katrina to the gulf coast states. North Carolina continues to identify and develop mission critical resource packages that can be rapidly deployed following an emergency. These resource packages will include private sector resources as needed.

In New York City, the Office of Emergency Management's new emergency operations center includes the private sector as an integral part of the city's response planning and operations. A variety of sectors, including financial services, building owners and managers, utilities and others, work alongside public sector agency representatives during an activation of the city's operations center. New York City's OEM has also developed a model credentialing program to facilitate access to restricted areas by key private sector personnel.

These are but a few examples of the work underway at the state and local levels to bring the private sector more formally into the nation's emergency response and recovery networks. It is important to note, that as recently as five years ago few such relationships existed, so in a very real sense significant progress has been, and continues, to be made.

Despite this tangible progress, a number of significant challenges remain, especially related to using private sector resources in interstate responses.

For example, only four states have statutory provisions that enable private sector resources to be used as "agents of the state" in out-of-state deployments – Delaware, Michigan, Maine and North Carolina. Other states have specific statutory or procurement policies that appear to preclude such arrangements.

This fact alone has forced the BMAC Task Force to rethink the overall strategy for how formally the private sector might be incorporated into the EMAC system. A fundamental premise of the EMAC legislation in each state is that personnel and equipment deployed out of state in response to a request received through EMAC from an impacted state must act as "agents" of the providing state. Other states have stringent restrictions on what "pre-event" contracts and arrangements can be negotiated with private sector entities and, in many cases, prohibitions against applying those contracts to a response into another state.

BENS is continuing an effort to identify the range of regulatory and statutory provisions that impact the use of private sector resources during major

emergencies. I would anticipate that at some point in the near future it will be necessary for this committee to consider whether there are federal statutory changes that are needed to address some of the identified barriers.

Next Steps to Integrate the Private Sector into Disaster Response

The BEMAC Task Force has identified several next steps that we believe will continue to advance the overall objective of defining a clearly understood process by which private sector resources can be mobilized across state boundaries during a major emergency. These next steps include:

- BENS, in cooperation with the U.S. Chamber of Commerce and the Business Roundtable will identify a Point of Contact (POC) for each of the Critical Sectors as identified by the Department of Homeland Security;
- NEMA will provide a briefing to the sector POCs on EMAC and will work with the BEMAC Task Force to promote the use of the POCs -- or other designated sector leads such as a trade or professional association – as the coordinating point for requests for private sector resources needed by an impacted state that are not available in the requesting state;
- NEMA will provide a document outlining "Best Practice" protocols and procedures developed by states for working with the private sector, and distribute the report to state emergency services directors as well as the Sector Coordinators;
- NEMA will work with the BEMAC Task Force to define and detail "mission critical" packages of resources projected to be needed during an emergency response and will promote the use of these packages by states requesting resources from the private sector;
- BEMAC Task Force members will participate in all NEMA/EMAC After-Action activities following the 2007 hurricane season to review progress made in utilizing private sector resources and identify actions to advance the overall initiative;
- The BEMAC Task Force will work to identify training exercises to enhance understandings of both the public and private sector on more effective use of private sector resources;
- NEMA, the BEMAC Task Force and the BENS legal and regulatory working group, will continue to more definitively understand the legal and procurement environment affecting use of private sector resources and develop recommendations that will address resolvable barriers;
- NEMA and the BEMAC Task Force will work with FEMA to address issues related to reimbursements for private sector resources and compensation for services used through an EMAC-like process; and

- The NEMA Board of Directors has included advancing the work of the BEMAC Task Force as part of their 2007-2008 work plan, ensuring that staff resources will continue to be devoted to this important work.

We believe that the steps outlined above will significantly advance the use of private sector resources by state and local entities as well as help clarify for the private sector a process that will be used in requesting resources.

The BEMAC Task Force believes strongly that states should be the primary focal point for this overall effort and that, like in the evolution of EMAC, it is important to take a few initial steps and gradually build more robust relationships and systems.

Clearly, FEMA needs to be an active partner in this process. We understand that FEMA has its own requirements and needs in using private sector resources. We look forward to working closely with the agency to ensure that these arrangements are clearly communicated to the states and the privates sector and that they are coordinated with the efforts being undertaken by NEMA/EMAC and the BEMAC Task Force.

Conclusion

The scale and variety of risks facing this nation from natural and man-made emergencies necessitate that public safety officials at all levels of government, as well as business representatives of key critical sectors, continue the effort to make full use of the resources of the nation in responding to and recovering from events that impact public safety, and continuity of operations in both the public and private sector. Only through such cooperation and partnerships can we accelerate individual and community economic restoration and recovery.

Thank you for the opportunity to share these thoughts with the members of the Committee.

Statement for the Record
Robert B. Stephan,
Assistant Secretary, Infrastructure Protection
National Protection and Programs Directorate
Department of Homeland Security

Before the

Committee on Homeland Security and Government Affairs
Subcommittee on State, Local and Private Sector Preparedness and Integration
United States Senate

Thursday, July 12, 2007
2:00 p.m.
Dirksen Senate Office Building, Room SD-342

Thank you, Chairman Pryor, Senator Sununu, and distinguished members of the Subcommittee. I appreciate this opportunity to address you on the role of the Department of Homeland Security (DHS) Office of Infrastructure Protection (OIP) in ensuring robust coordination with the private sector as we work together to protect our nation's critical infrastructure and key resources (CI/KR) and strengthen national CI/KR-related "all-hazards" incident management capabilities.

My staff and I are keenly aware of the importance of fully integrating and working with our private sector partners across our mission space. As a point of departure, it is important to note that the vast majority of our nation's critical infrastructure—approximately 85 percent—is owned and operated by private sector entities. Hence, our comprehensive work with the private sector represents a key component of our national CI/KR information sharing network and protective architecture. Both Congress and the President have recognized that, as a Nation, the full support, cooperation, and engagement of Government and private sector partners at all levels is required to prevent terrorist attacks, mitigate natural or manmade disasters, restore essential services in the aftermath of an incident, and maintain the American way of life.

I know you recently heard from R. David Paulison at the Federal Emergency Management Agency (FEMA) and Al Martinez-Fonts of the DHS Private Sector Office during Part One of this hearing. My office works very closely with both FEMA and the Private Sector Office in a collaborative approach to building and supporting this important public-private partnership. We have worked collaboratively to strengthen our incident management relationship with the private sector, building on important lessons learned during the 2005 hurricane season.

Our partnership with the private sector spans the diverse spectrum of the 17 CI/KR sectors identified in Homeland Security Presidential Directive-7 (HSPD-7). This partnership also extends to high-risk communities across the country, where we have focused a great deal of effort to bring together Federal, State and local government and private sector partners to conduct a variety of CI/KR-related activities such as vulnerability assessments, security planning, information sharing, best-practices exchanges, risk reduction, and incident management. This partnership, in fact, forms the operational core of our National Infrastructure

Protection Plan (NIPP) and its supporting Sector Specific Plans (SSPs) in each of the 17 CI/KR sectors.

I would like to take this opportunity today to provide you with specific examples of the progress the Department of Homeland Security has made over the past four years towards meeting the challenge of building and sustaining the comprehensive framework required to protect and enhance the resiliency of our nation's CI/KR in an all-hazards context. My remarks will focus on the following major topics:

- Roles and responsibilities of the Office of Infrastructure Protection;
- CI/KR protection framework detailed in the NIPP and its supporting SSPs;
- NIPP public-private sector partnership and information sharing model;
- NIPP risk management framework and protective programs that drive private sector coordination; and
- CI/KR dimension of our domestic incident management framework.

Roles and Responsibilities of the Office of Infrastructure Protection

Since its inception in March, 2003, the mission of the DHS Office of Infrastructure Protection has been clear. Our overall approach is focused on establishing and sustaining a risk-based, unified program to protect and enhance the resiliency of our nation's CI/KR. The key to this approach is the successful integration of diverse authorities, resources, and capacities across a broad universe of functional agencies, governmental jurisdictions, and private industries to achieve a "layered defense" of physical protection, cyber security, and resiliency within the 17 CI/KR sectors.

This is a long-term effort that involves comprehensive government and private sector collaboration inside and outside of regulatory space at various levels across our national risk landscape. For its part, the private sector has made substantial investments to strengthen physical and cyber security, boost resiliency, increase redundancy, and develop contingency plans since the September 11th attacks. State and local agencies have also stepped up to the plate in many important ways to strengthen their ability to support the CI/KR protection mission within their jurisdictions. Supporting these efforts, the Department has provided nearly $2 billion in CI/KR-targeted risk-based grant funding – including $445 million this year – to deter threats, reduce vulnerabilities, minimize consequences, and build resiliency across our nation's most at-risk CI/KR.

The basic charter of the Office of Infrastructure Protection is to provide the coordinating leadership required at the national level to build and sustain a very complex, dynamic, and diverse protection partnership that drives unity of effort across the 17 CI/KR sectors. In our OIP FY08-13 Strategic Plan, we have identified six primary goals essential to implementing our national mission:

- Build and sustain effective CI/KR partnerships and coordination mechanisms;

- Understand and share risk and other information about terrorist threats and other hazards to the nation's CI/KR;
- Build and implement a sustainable, national CI/KR risk-management program;
- Ensure efficient use of resources for CI/KR risk management;
- Provide a foundation for continuously improving national CI/KR preparedness; and
- Promote a culture of organizational excellence and a quality work environment that values and supports the workforce.

CI/KR Protection Framework Detailed in the NIPP and Its Supporting SSPs

The guiding force behind our strategic planning and resource allocation activities is the National Infrastructure Protection Plan, or NIPP. I am pleased to report that we marked a significant milestone on June 30th of this year–the first anniversary of the issuance of the NIPP, our strategic national blueprint for the CI/KR mission area that was, in fact, developed through the public-private partnership framework. The achievements that I will discuss with you today are a direct result of the commitment, dedication, and teamwork that characterizes this framework.

Through the NIPP, we now have a unified national game plan and an ever expanding arsenal of tools with which to implement our mission. The NIPP establishes the overall risk-based construct that defines the unified approach to protect and enhance the resiliency of the nation's CI/KR in an all-hazards context. This construct applies to "steady-state" risk reduction activities across the sectors and also sets the stage for important CI/KR-related response and recovery activities under the National Response Plan (NRP).

Organizationally, the heart of the NIPP is the sector partnership model that establishes Sector Coordinating Councils (SCCs), Government Coordinating Councils (GCCs), and cross-sector coordinating councils to create an integrated national framework for CI/KR preparedness, protection, response and recovery across sectors and levels of government. This partnership model also forms the backbone of the networked approach to sharing information. A robust system for information sharing provides for multidirectional CI/KR-related exchanges of actionable intelligence, alerts, warnings, and other information between the various NIPP partners, including: Federal agencies, State and local agencies, CI/KR owners/operators, and sector-based information-sharing entities.

The NIPP partnership model encourages CI/KR owners and operators to create or identify an SCC as the principal entity for coordinating with the government on a wide range of CI/KR protection activities and issues. SCCs are self-run and self-governed; specific membership varies from sector to sector, reflecting the unique composition of each sector. The guiding principle for SCCs is that membership is structured to be representative of a broad base of owners, operators, associations, and other entities – both large and small – within a sector.

GCCs serve as the government counterpart for each sector to enable interagency and cross-jurisdictional coordination. GCCs are comprised of representatives from across various levels of government and functional disciplines as appropriate to the security landscape of each sector. Each GCC is chaired by a representative from the designated Federal Sector-Specific Agency and co-chaired by myself, as the Assistant Secretary for Infrastructure Protection.. Together, the

SCCs and GCCs provide a forum through which NIPP security partners may engage in a broad spectrum of activities, such as: security planning, policy coordination, exercise planning, risk methodology coordination, implementation of protection initiatives, information sharing, and incident management.

The "glue" that binds this partnership together is the NIPP "value proposition" that articulates guiding principles for coordination and cooperation between government at all levels and the private sector. In accordance with these principles, DHS is committed to:

- Providing owners and operators with timely, accurate, and actionable all-hazards information;
- Ensuring that owners and operators are engaged at senior executive and operational levels in key planning, policy, requirements, and resource allocation discussions;
- Articulating the benefits of a risk-based, cross-sector approach to preparedness, resilience, and protection;
- Working with owners and operators to clearly establish risk-based priorities for prevention, protection, and recovery;
- Providing specialized technical and planning expertise to support CI/KR-related preparedness, protection, and recovery; and
- Coordinating with CI/KR owners and operators on priorities, risk assessments, mitigation, and restoration and recovery activities in the context of incident management.

The finalization and release of the NIPP Sector-Specific Plans (SSPs) in May of this year represents another important milestone and illustrates the effectiveness of the NIPP Partnership Framework, which is, interestingly enough, a purely voluntary structure. Developed under the umbrella of this Framework, the SSPs represent adaptations of the NIPP baseline risk analysis and risk management approach, governance structure, and information sharing network as tailored to the specific needs and requirements of each of the 17 CI/KR sectors. This undertaking represents the first time that the Government and private sector have come together on such a large scale – literally across every major sector of our economy – to develop joint plans for how to protect and ensure the resiliency of our CI/KR against both terrorist incidents and natural disasters.

The development of the SSPs was, in fact, a comprehensive and dynamic undertaking that brought together thousands of public and private sector organizations across the 17 CI/KR sectors. The direct involvement of CI/KR owners and operators, State and local government agencies, trade associations, professional organizations, and other security partners was inherent to this process. As part of this effort, my office conducted six technical assistance sessions during the 180-day SSP development process to address selected topics such as the incorporation of research and development requirements, information sharing networks and protocols, and the sharing of best practices across sectors. Each sector devised its own preferred approach for developing its plan and was required to ensure inclusion of a full slate of sector security partners. Many sectors conducted multiple review cycles, resulting in a robust consideration of sector partner comments and, ultimately, a more complete and inclusive end product. The overall magnitude of comments across the sectors was indicative of the degree of interest in and the importance of this effort. An estimated 10,000 individual comments were received and

adjudicated, which is roughly the same number of comments processed during the development of the NIPP Base Plan.

In a series of parallel undertakings, we are also leveraging the NIPP Sector Coordinating Council structure to develop sector guidelines for pandemic influenza preparedness, establish CI/KR protection research/development and modeling/analysis requirements, build a national CI/KR protection awareness and training program, and provide for expanded private sector participation in the DHS National Exercise Program (to include the upcoming Top Officials (TOPOFF) 4 exercise).

NIPP Public-Private Sector Partnership and Information Sharing Model

The NIPP partnership framework is enabling marked progress in another important area—information sharing. In accordance with the NIPP, we are currently implementing a networked approach to information sharing that constitutes a dramatic shift from a strictly hierarchical approach, that is, the Federal government sharing information down.. This networked approach allows distribution and access to information both horizontally and vertically using secure networks and coordination mechanisms, allowing information sharing and collaboration within and among sectors. It also enables multi-directional information sharing between government and industry that focuses, streamlines, and reduces redundant reporting to the greatest extent possible. Security partners are finding immediate value in tactical activities that incorporate sector-specific subject matter expertise. These processes are enabling the integration of the private sector security partners, as appropriate, into the intelligence cycle and National Common Operating Picture. Moreover, sector security partners are becoming more confident that the integrity and confidentiality of their sensitive information can and will be protected and that the information-sharing process can produce actionable information regarding CI/KR threats, incidents, vulnerabilities, and potential consequences.

Our efforts to enhance the sharing of information related to terrorism with the owners and operators of CI/KR have been integrated into broader efforts to establish the Information-Sharing Environment (ISE) as directed by the President in accordance with the Intelligence Reform and Terrorism Prevention Act of 2004. The purpose of the ISE is to measurably improve information sharing between and among Federal, State, local, and tribal governments; and between government agencies and private sector entities. In recognition of the important work underway in this area under the NIPP framework, the Program Manager of the ISE, in coordination with the Information Sharing Council, has officially designated the NIPP Partnership Framework coordinated through the Office of Infrastructure Protection as the Private Sector Subcommittee of the Information Sharing Council. In this role, the NIPP Partnership Framework provides an avenue for the private sector to engage in ISE-related policy, planning, and operational coordination, as well as a forum for identifying and satisfying information requirements originating from private sector security partners.

The CI/KR owners and operators utilize a number of mechanisms that facilitate the flow of information, mitigate obstacles to voluntary information sharing by CI/KR owners and operators, and provide feedback and continuous improvement regarding structure and process. These include the SCCs/GCCs, National Infrastructure Coordinating Center (NICC), Sector-level

Information Sharing and Analysis Centers (ISACs), OIP Sector Specialists, OIP Protective Security Advisors, DHS Homeland Infrastructure Threat and Risk Analysis Center (HITRAC), and State and Major Urban Area Fusion Centers. These mechanisms accommodate a broad range of sector cultures, operations, and risk management approaches and recognizes the unique policy and legal challenges for full two-way sharing of information between the CI/KR owners and operators and government, as well as their unique requirements for efficient operational processes.

NIPP Risk Management Framework and Protective Programs that Drive Private Sector Coordination

During a situation or crisis, the ability to share concise and focused information with all those who need access to it is essential. To accomplish this end, the National Infrastructure Coordinating Center (NICC) was created as our 24/7 watch center focal point for coordination and communication with the CI/KR sectors. The NICC leverages the Homeland Security Information Network—Critical Sectors (HSIN-CS) as a mechanism to push information to private sector CI/KR owner-operators. The NICC has posted more than 800 threat assessments, situation reports, daily updates, and analysis documents within the past year, including pre-season CI/KR hurricane impact analyses produced by OIP's National Infrastructure Simulation and Analysis Center (NISAC).

Another important advancement in our relationship with the private sector is the establishment of the Homeland Infrastructure Threat and Risk Analysis Center (HITRAC), an infrastructure-intelligence fusion center that we operate jointly with the DHS Office of Intelligence and Analysis (I&A). Working in partnership with members of the U.S. Intelligence Community and national law enforcement agencies, HITRAC analyzes and monitors risks to domestic CI/KR, allowing our Office to provide actionable assessments and risk reduction recommendations to our sector security partners at both the classified and unclassified levels. Access to classified information and discussions is permitted through a security clearance sponsorship program in which we have provided SECRET-level clearances to more than 900 private-sector officials across the 17 CI/KR sectors.

Through HITRAC and the NICC, private sector security partners receive a thorough combination of real-time threat, situation, and status information and analyses which, in turn, is used to inform security and operational planning, resource investments, and key risk mitigation activities. Private sector liaison personnel, on-call subject matter experts, and other organizations – including, but not limited to, the National Coordinating Center for Telecommunications, SCCs, GCCs, and ISACs – are utilized by HITRAC and the NICC in order to help inform comprehensive analyses of all-source information, and provide timely threat and warning products as well as a variety of more strategic level assessment products.

Collaborating with other key stakeholders through the NIPP Partnership Framework is fundamental to the success of numerous important national CI/KR-related risk reduction initiatives—to include important "boots-on-the-ground" activities—that DHS has implemented during the last four years. Examples of these activities include following:

Comprehensive Reviews – This initiative involves a structured, joint analysis of Federal, State, local, and private sector capabilities needed to enhance the security of our highest-risk national CI/KR. Recommendations to mitigate the effects of a potential terrorist attack, natural disaster, or other emergency on these infrastructures as well as an ability to target Federal CI/KR protection grants against gaps identified are provided through this program. To date, we have conducted 64 comprehensive reviews involving both the Chemical and Nuclear Sectors. The Chemical Sector Comprehensive Review Team conducted analyses of six regions that included nine states and Federal grant funding of $25 million. The Nuclear Sector Comprehensive Review Team conducted 58 comprehensive reviews that provided the basis for additional security improvements within the Nuclear Sector through the Buffer Zone Protection Program.

Buffer Zone Protection Program (BZPP) – The BZPP is a DHS-administered grant program designed to help local law enforcement and CI/KR owners and operators increase security within the "buffer zone," the area outside of a facility that can be used by an adversary to conduct surveillance or launch an attack. This program provides a coordinated process to identify and assess vulnerabilities, conduct security planning, implement preparedness activities, coordinate protective measures, and obtain mitigation equipment needed to enhance security. More than 2,200 BZPP site visits, 181 planning workshops, and 176 technical assistance visit engagements have taken place since 2004 in locations around the country. DHS has distributed approximately $190 million in grants to our State and local law enforcement security partners in order to improve the overall security posture of these high-risk areas and to refine and strengthen locally generated CI/KR protection plans.

Site Assistance Visits (SAVs) – The SAV program provides a collaborative process for conducting information-gathering visits in support of several key objectives, such as gaining a better understanding and prioritization of CI/KR vulnerabilities and increasing owner and operator awareness of threats and vulnerabilities. These visits are conducted jointly by DHS, other Federal, State, and local government entities, and CI/KR owners and operators. Through this program, we provide CI/KR owners and operators with options for increasing their ability to detect and prevent terrorist attacks and recommendations for reducing infrastructure vulnerability. Information derived from these visits is used to produce Common Vulnerabilities, Potential Indicators of Terrorist Activity, and Protective Measures reports that are available to Federal, State, local, tribal, and private sector partners through our information-sharing network. In the last two years, we have conducted a total of 700 Site Assistance Visits, with an aggressive schedule for many more through the end of FY 2007 and into FY 2008.

Protective Security Advisors (PSAs) – PSAs represent a critical in-place "boots on the ground" capability in high-risk areas around the country. Although we do a great deal of planning and coordination here in Washington, D.C., CI/KR-related program implementation, partnership interaction, and performance feedback are more appropriately driven home at the local level. Recognizing this fact, DHS has permanently stationed 78 PSAs strategically throughout the country to enhance CI/KR protection efforts and stakeholder interaction. These trained protective security experts foster, build, and maintain partnerships with State, local, and tribal governments, community leaders, CI/KR owners and operators, and local-level businesses on a daily basis. PSAs coordinate requests from CI/KR owners and operators for services and resources, including Soft Target Awareness Courses (STACs), Surveillance Detection (SD)

training, vulnerability assessments, security planning sessions, and technical assistance visits. To date, PSAs have conducted more than 15,000 liaison visits with State, local, and private sector partners. They have also provided support to the 2,200 Buffer Zone Protection Program planning efforts; 6 Chemical Sector Comprehensive Reviews, 54 Nuclear Sector Comprehensive Reviews, and participated in approximately 500 Site Assistance Visits. .

PSAs are the first Office of Infrastructure Protection personnel to respond to incidents within their area of responsibility. PSAs provide crucial situational awareness during times of crisis or special events, including Hurricanes Katrina, Ophelia, Rita, and Wilma; the Virginia Tech shootings; and the ongoing flood and wildfire events in the Midwest and Pacific Coast. They are also engaged in security planning and situational awareness activities supporting special events such as the Super Bowl, Indianapolis 500, 2010 Olympics, and so forth.

Multi-Jurisdiction Improvised Explosive Device (IED) Security Plans – The Multi-Jurisdiction IED Security Planning process assists security partners in high-risk urban areas and other locations throughout the United States in developing thorough bombing prevention and response plans. These plans are intended to integrate assets and capabilities from multiple jurisdictions and emergency service disciplines. As part of this program, to date we have conducted more than 17 security plan development sessions for high risk port facilities around the country. These efforts have focused on enhancing port security preparedness for a potential terrorist attack using Underwater Hazardous Devices (UHDs). The multi-jurisdictional IED Security Planning workshop provides participants with a comprehensive, tailored annex to the Area Maritime Security Plan that details the prevention of, response to, and recovery from, a UHD attack.

Technical Resource for Incident Prevention (TRIPwire) – TRIPwire is an online, collaborative, information-sharing network designed to support bomb squads and other law enforcement officials. It provides users with information about current terrorist bombing tactics, techniques, and procedures, including IED design and placement. By combining expert analysis and reports with relevant documents, images, and videos gathered directly from terrorist sources, TRIPwire helps operators anticipate, identify, and prevent bombing incidents. TRIPwire is provided via a secure, restricted access Internet portal free of charge to qualified bombing prevention and law enforcement community personnel. TRIPwire currently has more than 1,800 users, including 566 certified bomb technicians, and has the potential to reach more than 500,000 emergency services personnel. Current users represent 40 Federal departments and agencies, 28 military units, 365 State and local agencies, and 35 private sector companies and organizations. Since June 2006, TRIPwire has received nearly 4,000,000 site hits.

Soft Target Awareness (STAC) and Surveillance Detection (SD) Training – The STAC is a week-long course that provides private sector facility managers, supervisors, and security and safety personnel with a venue to receive and share baseline terrorism awareness, prevention, and protection information and is intended to enhance individual and organizational security awareness. SD Training is a three-day course that provides a guideline for mitigating risks to CI/KR through developing, applying, and employing protective measures and the creation of a surveillance detection plan. OIP has provided 284 STACs across 71 cities and 97 SD Trainings within a wide variety of locations around the country.

NIPP Awareness Level Training Program – Since being put online in late-December 2006, this web-based training program has been accessed by more than 1,000 security partners each month. Developed in coordination with the FEMA Emergency Management Institute, this program offers NIPP training free of charge to all security partners, including private sector owners and operators. Recently, a classroom version of the course was developed, and participants have the option of completing either the web-based training program or the classroom program for continuing credit. Companion training videos have also been created for use across various venues to explain the NIPP; each video includes testimonials from several key private sector partners.

CI/KR Dimension of Our Domestic Incident Management Framework

In the aftermath of the 2005 hurricane season, we have worked very closely with Federal, State, and local incident managers and private sector entities to build out a robust CI/KR incident management framework and operational capability. We have collaborated extensively with the National Operations Center (NOC) and now provide direct day-to-day representation and coordination of key CI/KR functional elements for the NOC. We also maintain full-time OIP representation on the DHS Incident Management Planning Team and at the FEMA National Response Coordination Center (NRCC). This representation ensures that CI/KR inputs, interests, and concerns are accurately presented and included in the development of both the National Common Operating Picture and Federal Interagency Contingency Plans – based on the 15 National Planning Scenarios – through detailed CI/KR annexes. These OIP representatives also ensure the incorporation of CI/KR interests into other contingency plans, such as hurricane season preparedness plans, and NRP activation for incidents that require Federal involvement.

In another area, OIP is engaged in multiple planning and information-sharing initiatives with CI/KR owners and operators to ensure the integrity of the nation's CI/KR in the event of an influenza pandemic. These efforts support the DHS overarching responsibility for coordination of Federal response activities. The Pandemic Influenza CI/KR Preparedness, Response, and Recovery Guide was completed in 2006 and posted to the www.pandemicflu.gov and www.ready.gov websites. Continuing this effort, we are now actively engaged in additional activities to stimulate and support CI/KR pandemic preparedness. A comprehensive process to develop 17 sector-specific guidelines in collaboration with each of the SCCs and GCCs is currently underway. These guidelines, which are expected to be completed by early fall, will provide comprehensive, sector-unique planning information for our security partners. Once completed, these guidelines will be posted to Federal and industry websites and widely disseminated to businesses. Additionally, over the past year, we conducted workshops and forums to identify issues and gaps in CI/KR pandemic influenza planning. Multiple pandemic influenza preparedness workshops are planned over the next 12 months to continue the dialogue between CI/KR owners and operators and their community, State, local, tribal, Territorial, and Federal partners.

In support of our evolving incident management roles and responsibilities, OIP is focusing a great deal on training and exercise programs to test our exiting coordination capabilities, information sharing network, and overall readiness. We have significantly raised our level of readiness to provide CI/KR support for incident management through our training and exercise

programs, each of which is fully compliant with the Homeland Security Exercise and Evaluation Program (HSEEP). The CI/KR sectors are actively planning for participation in the DHS-led TOPOFF 4 full-scale national exercise in October 2007. This exercise will test our analysis and coordination processes and provide a venue for government and private sector leaders to verify and validate our preparations for a catastrophic terrorist attack. Several hundred private sector partners participated in the TOPOFF 3 exercise in 2005, and we expect even greater participation for the upcoming TOPOFF 4 event.

In addition to OIP and DHS specific readiness, OIP also focuses on Sector-Based readiness activities. The NICC recently disseminated a series of documents to the CI/KR Sectors to support sector preparedness efforts for the 2007 hurricane season. These products included: 1) the 2007 scenario-driven NISAC hurricane impact analysis products that address potential CI/KR impacts in a number of high-risk geographic regions and 2) updated protocols for incident-related CI/KR sector impact assessment and status reporting, information-sharing, and requests for information and assistance. Additionally, the NICC hosted two training workshops for the Federal Sector-Specific Agencies to refine public-private sector reporting processes prior to the 2007 hurricane season. The NICC also conducts monthly reporting drills with the SSAs and more frequent drills with the National Operations Center (NOC).

Finally, in response to significant CI/KR security events such as the foiled airline bombing plot in the United Kingdom last August, the recent JFK Airport bombing plot, and the recent attempted bombing events in London and Glasgow, OIP convened conference calls with the SCCs to share critical information and recommendations regarding these situations as they developed with our private sector partners.

Currently, we are finalizing OIP's long-term strategy for continued program growth and evolution. This effort is being conducted in tandem with the Sector Annual Reporting process under the NIPP. Our goal is to continue our risk-based approach to CI/KR protection, tailored to the needs and requirements of the 17 CI/KR sector. As we move into the future, the NIPP Partnership Framework and the thousands and thousands of security partners it brings together will continue to drive our national approach. No one can predict the future with 100% accuracy but certain things are a given—technology, the ways CI/KR owners and operators do business, and their supply chain dependencies will evolve, and vulnerabilities and consequences will change accordingly. In effect, we can count on our risk calculation changing in a dynamic fashion over time. Another fact is very clear—we know that we face a clever, flexible, patient, and determined terrorist adversary. The path forward provided by the NIPP, the SSPs, and the NIPP Partnership Framework will continue to serve us well and allow us to act collaboratively to adapt to a dynamic risk environment and achieve national unity of effort.

Success over time means making commitments and following through with them. We will approach our collaborative implementation of the NIPP and SSPs with this in mind and continue to refine and enhance our solid relationship with the private sector. I will leave you with one more important observation—the more we utilize the Sector Partnership Framework for the appropriate purposes, the stronger and more effective it gets. We continue to incorporate lessons learned from interactions on various relevant issues that enable continuous improvement and adaptation of partnership communication and coordination.

The NIPP and its supporting SSPs chart the path forward for continuous improvement in the security and resiliency of our critical infrastructure. Continued support of the focused activities of OIP in concert with all of our CI/KR partners will help ensure our preparedness in this critical mission area.

Thank you for this important opportunity to discuss the CI/KR protection mission area and the public-private sector partnership framework that lies at its core. I would also like to thank you for your continued support and dedication to the success of this vital component of the overarching homeland security mission. I would be happy to answer any questions that you may have at this time.

United States Government Accountability Office

GAO

Testimony before the Subcommittee on State, Local, and Private Sector Preparedness and Integration, Committee on Homeland Security and Government Affairs, U.S. Senate

For Release on Delivery
Expected at 2:00 p.m. EDT
Thursday, July 12, 2007

CRITICAL INFRASTRUCTURE

Sector Plans Complete and Sector Councils Evolving

Statement of Eileen R. Larence, Director
Homeland Security and Justice Issues

GAO-07-1075T

July 12, 2007

GAO
Accountability·Integrity·Reliability

Highlights

Highlights of GAO-07-1075T, a testimony before the Subcommittee on State, Local, and Private Sector Preparedness and Integration, Committee on Homeland Security and Government Affairs, U.S. Senate

CRITICAL INFRASTRUCTURE

Sector Plans Complete and Sector Councils Evolving

Why GAO Did This Study

As Hurricane Katrina so forcefully demonstrated, the nation's critical infrastructures—both physical and cyber—have been vulnerable to a wide variety of threats. Because about 85 percent of the nation's critical infrastructure is privately owned, it is vital that public and private stakeholders work together to protect these assets. The Department of Homeland Security (DHS) is responsible for coordinating a national protection strategy and has promoted the formation of government and private councils for the 17 infrastructure sectors as a collaborating tool. The councils, among other things, are to identify their most critical assets, assess the risks they face, and identify protective measures in sector-specific plans that mesh with DHS's National Infrastructure Protection Plan (NIPP).

This testimony is based primarily on GAO's July 2007 report on the sector-specific plans and the sector councils. Specifically, it addresses (1) the extent to which the sector-specific plans provide a framework for the protection of critical infrastructure, (2) the value of the plans and DHS's review process, and (3) the key success factors and challenges that the representatives encountered in establishing and maintaining their councils. In conducting the previous work, GAO reviewed 9 of the 17 draft plans and conducted interviews with government and private sector representatives of the 18 councils, 17 government and 15 private sector.

www.gao.gov/cgi-bin/getrpt?GAO-07-1075T.

To view the full product, including the scope and methodology, click on the link above. For more information, contact Eileen Larence at (202) 512-8777 or larencee@gao.gov..

What GAO Found

Although the nine sector-specific plans GAO reviewed generally met NIPP requirements and DHS's sector-specific plan guidance, eight did not describe any incentives the sector would use to encourage owners to conduct voluntary risk assessments, as required by the NIPP. Most of the plans included the required elements of the NIPP risk management framework. However, the plans varied in how comprehensively they addressed not only their physical assets, systems, and functions, but also their human and cyber assets, systems and functions, a requirement in the NIPP, because the sectors had differing views on the extent to which they were dependent on each of these assets. A comprehensive identification of all three categories of assets is important, according to DHS plan guidance, because it provides the foundation on which to conduct risk analyses and identify appropriate protective actions. Given the disparity in the plans, it is unclear the extent to which DHS will be able to use them to identify security gaps and critical interdependencies across the sectors. DHS officials said that to determine this, they will need to review the sectors' annual reports.

Representatives of the government and sector coordinating councils had differing views regarding the value of sector-specific plans and DHS's review of those plans. While 10 of the 32 council representatives GAO interviewed reported that they saw the plans as being useful for their sectors, representatives of eight councils disagreed because they believed the plans either did not represent a partnership among the necessary key stakeholders, especially the private sector or were not valuable because the sector had already progressed beyond the plan. In addition, representatives of 11 of the 32 councils felt the review process was too lengthy, but 8 thought the review process worked well. The remaining council representatives did not offer views on these issues.

As GAO reported previously, representatives continued to report that their sector councils had preexisting relationships that helped them establish and maintain their sector councils. However, seven of the 32 representatives reported continuing difficulty achieving and maintaining sector council membership, thus limiting the ability of the councils to effectively represent the sector. Eleven council representatives reported continuing difficulties sharing information between the public and private sectors as a challenge, and six council representatives expressed concerns about the viability of the information system DHS intends to rely on to share information about critical infrastructure issues with the sectors or the effectiveness of the Protected Critical Infrastructure Information program—a program that established procedures for the receipt, care, and storage of information submitted to DHS. GAO has outstanding recommendations addressing this issue, with which DHS generally agreed and is in the process of implementing.

Mr. Chairman, Ranking Member and Members of the Subcommittee:

Thank you for inviting us to participate in today's hearing on infrastructure protection issues. In 2005, Hurricane Katrina devastated the Gulf Coast, damaging critical infrastructure, such as oil platforms, pipelines, and refineries; water mains; electric power lines; and cellular phone towers. The infrastructure damage and resulting chaos disrupted government and business functions alike, producing cascading effects far beyond the physical location of the storm. In 2004, authorities thwarted a terrorist plot to target financial institutions in New York. In 2005, suicide bombers struck London's public transportation system, disrupting the city's transportation and mobile telecommunications infrastructure. Our nation's critical infrastructures and key resources—including those cyber and physical assets essential to national security, national economic security, and national public health and safety—continue to be vulnerable to a wide variety of threats. Because the private sector owns approximately 85 percent of the nation's critical infrastructure and key resources—banking and financial institutions, telecommunications networks, and energy production and transmission facilities, among others—it is vital that the public and private sectors form effective partnerships to successfully protect these assets.[1]

The Department of Homeland Security (DHS) is a key player in these partnerships. The Homeland Security Act of 2002 created DHS, giving the department wide-ranging responsibilities for leading and coordinating the overall national critical infrastructure protection effort.[2] The act required DHS to (1) develop a comprehensive national plan for securing the nation's critical infrastructures and key resources and (2) recommend measures to protect critical infrastructure and key resources. Homeland Security Presidential Directive 7 (HSPD-7) further defined critical infrastructure protection responsibilities for DHS and those federal agencies—known as sector-specific agencies—responsible for particular

[1]"Critical infrastructure" are systems and assets, whether physical or virtual, so vital to the United States that their incapacity or destruction would have a debilitating impact on national security, national economic security, national public health or safety, or any combination of those matters. Key resources are publicly or privately controlled resources essential to minimal operations of the economy or government, including individual targets whose destruction would not endanger vital systems but could create a local disaster or profoundly damage the nation's morale or confidence. For purposes of this statement, we will use the term "critical infrastructure" to also include key resources.

[2]See Pub. L. No. 107-296, 116 Stat. 2135 (2002).

industry sectors, such as transportation, energy, and communications. Under HSPD-7, DHS is to establish uniform policies, approaches, guidelines, and methodologies to help ensure that critical infrastructure within and across the 17 infrastructure sectors is protected.[3] The directive further promotes the use of a risk management approach to coordinate protection efforts. This approach includes using risk assessments to set priorities for protective measures by the department; sector-specific agencies; tribal, state, and local government agencies and authorities with critical assets and resources in their jurisdiction; owners and operators of these assets; and other entities.

In addition, HSPD-7 required DHS to develop a comprehensive and integrated plan for securing the nation's critical infrastructures that outlines national protection goals, objectives, milestones, and key initiatives necessary to fulfilling these responsibilities. In response, DHS developed the National Infrastructure Protection Plan (NIPP). Issued in June 2006, the NIPP is a base plan that is to serve as a road map for how DHS and other relevant stakeholders, such as owners and operators of key critical infrastructure, should use risk management principles to prioritize protection activities within and across sectors in an integrated, coordinated fashion. In particular, the NIPP—along with more detailed guidance issued by DHS—required the individual sector-specific agencies, working with relevant government and private representatives, to submit sector-specific plans to DHS by the end of December 2006. The plans, which were released on May 21, 2007, were to establish the means by which the sectors will identify their critical assets, assess risks of terrorist attacks or other hazards to these assets, assess and prioritize those assets which have national significance, and develop protective measures for the sectors. The NIPP also requires that sector-specific agencies develop annual reports that discuss the sectors' status in implementing the plans. According to the NIPP, DHS is to use these individual plans and reports to develop an annual cross-sector report, due each September, that evaluates whether gaps exist in the protection plans and actions to be taken to protect critical infrastructures on a national level. If gaps exist, DHS is to work with the sectors to address them.

[3]These infrastructure sectors include agriculture and food; banking and finance; chemical; commercial facilities; commercial nuclear reactors, materials, and waste; communications; dams; defense industrial base; drinking water and water treatment systems; emergency services; energy; government facilities; information technology; national monuments and icons; postal and shipping; public health and health care; and transportation systems.

To protect critical infrastructure, the NIPP describes a partnership model as the primary means of coordinating government and private efforts. For each of the 17 sectors, the model requires formation a government coordinating council—composed of representatives of federal, state, local, or tribal agencies with purview over critical assets. The model encourages voluntary formation of a sector coordinating council—composed of representative owner-operators of these critical assets (some of which may be state or local agencies) or their respective trade associations. There are a total of 32 coordinating councils, 17 government and 15 private sector.[4] These councils create the structure through which respective groups from all levels of government and the private sector are to collaborate in developing the sector-specific plans and implementing efforts to protect critical infrastructure. The sector coordinating councils are envisioned as a primary point of contact for government to plan the entire range of infrastructure protection activities unique to the sector. In addition, the NIPP also identified cross-sector councils that are to promote coordination, communications, and the sharing of key practices across the sectors.

This statement discusses (1) the extent to which the sector-specific plans meet NIPP and DHS requirements, (2) the government and sector coordinating council members' views on the value of the plans and DHS's review process, and (3) the key success factors and challenges that sector representatives reported they encountered in establishing and maintaining their councils. My comments today are based on our July 2007 report on the sector-specific plans and sector councils.[5] Our July report was based on a review of the NIPP as well as the sector-specific plan guidance to ascertain the elements required in the plans. We also obtained and reviewed 9 of the 17 draft plans against the criteria in the NIPP and plan guidance.[6] For more detail on the criteria we used, see appendix I. We

[4]The government facilities and the national monuments and icons sectors do not have sector councils because they do not have private sector counterparts.

[5]GAO, *Critical Infrastructure Protection: Sector Plans and Sector Councils Continue to Evolve*, GAO-07-706R (Washington, D.C.: July 10, 2007).

[6]We selected the nine plans to obtain a range of plans based on sector characteristics, such as the maturity—sectors with pre-existing relationships and a history of working together—and diversity of the sector. The plans we reviewed were banking and finance, communications, defense industrial base, energy, public health and healthcare, information technology (IT), national monuments and icons, transportation systems, and drinking water and water treatment systems. According to DHS officials, differences between these draft plans and the final plans issued on May 21, 2007, were insignificant.

conducted structured interviews with representatives of the 17 government coordinating councils and the 15 sector coordinating councils to obtain views on the value of the plans and the review process as well as the key success factors and challenges the sectors reported that they had encountered in establishing and maintaining their councils. These interviews were conducted with lead sector-specific agency representatives for the 17 sectors: the departments of Agriculture, Defense, Energy, Health and Human Services, Homeland Security,[7] the Interior, and the Treasury and the Environmental Protection Agency, as well as with the chairs, co-chairs, or steering committee members of the 15 sector coordinating councils. We conducted our work in accordance with generally accepted government auditing standards.

In Summary

Although the nine sector-specific plans we reviewed generally met NIPP requirements and DHS's sector-specific plan guidance, eight plans did not address incentives the sectors would use to encourage owners to conduct risk assessments and some plans were more comprehensive than others when discussing their physical, human, and cyber assets, systems, and functions. Most of the plans included the required elements of the NIPP risk management framework, such as security goals; and the methods the sectors expect to use to prioritize infrastructure as well as to develop and implement protective programs and assess threats, risks, and vulnerabilities.[8] However, some plans were more developed and comprehensive, depending on the maturity of the sector and on how the sector defines its assets and functions. While all of the plans described the threat analyses that the sector conducts, eight of the plans did not describe any incentives the sector would use to encourage owners to conduct voluntary risk assessments, as required by the NIPP. These incentives are important because a number of the industries in the sectors are privately owned and not regulated, and the government must rely on voluntary compliance with the NIPP. DHS officials said that the variance in the plans can primarily be attributed to the levels of maturity and cultures of the sectors, with the more mature sectors—sectors with preexisting relationships and a history of working together—generally

[7]DHS is the sector-specific agency for 10 sectors: information technology; communications; transportation systems; chemical; emergency services; commercial nuclear reactors, material, and waste; postal and shipping; dams; government facilities; and commercial facilities.

[8]See appendix I for the required elements on which we reviewed the plans.

having more comprehensive and complete plans than more newly established sectors without similar prior relationships. The plans also varied in how comprehensively they addressed not only their physical assets, systems, and functions,[9] but also their human and cyber assets, systems, and functions, a requirement in the NIPP, because the sectors reported that they had differing views on the extent to which they were dependent on each of these assets. A comprehensive identification of all three categories of assets is important, according to DHS sector-specific plan guidance, because such analysis provides the foundation on which to conduct risk analyses and identify the appropriate mix of protective programs and actions that will most effectively reduce the risk to the nation's infrastructure. Yet, only one of the plans—drinking water and water treatment systems—included all three categories of assets. For example, because the communications sector limited its definition of assets to networks, systems, and functions, it did not, as required by DHS plan guidance, discuss how human assets fit into existing security projects or are relevant to fill the gaps to meet the sector's security goals. DHS's Office of Infrastructure Protection officials acknowledged the differences in how comprehensive the plans are, but said that these initial plans are only a first step and that they will work with the sectors to address differences in future updates. Given the disparity in the plans, however, it is unclear the extent to which DHS will be able to use them at this point to identify security gaps and critical interdependencies across the sectors in order to plan future protective measures. From reviewing these plans, it is also unclear how far along each sector actually is in identifying assets, setting priorities, and developing activities to protect key assets. DHS officials said that to determine this, they will need to review the sectors' annual progress reports, due this month, that are to provide additional implementation information.

Representatives of the government and sector coordinating councils had differing views regarding the value of sector-specific plans and DHS's review of those plans. While 10 of the 32 council representatives we interviewed reported that they saw the plans as useful for the sector, representatives of eight councils disagreed because they believed the plans either did not represent a partnership among the necessary key stakeholders, especially the private sector, or were not valuable because

[9]In the context of the NIPP, a "system" is a collection of assets, resources, or elements that perform a process that provides infrastructure services to the nation. A "function" is defined as the service, process, capability, or operation performed by specific infrastructure assets, systems, or networks.

the sector had already done so much work on its own and had progressed beyond the plan. For example, the government facilities council representative said that the plan was useful because relationships across the sector were established during its development that have resulted in enhanced coordination of previously disjointed security efforts. DHS's Office of Infrastructure Protection officials agreed that the main benefit of the plans was that the process of developing them helped the sectors establish relationships between the private sector and the government and among private sector stakeholders. In contrast, the representative from the nuclear reactors, materials, and waste sector's coordinating council said that because the sector's security has been robust for a long time, the plan only casts the security of the sector in a different light. Also, the drinking water and water treatment sector representative said that the plan did not provide added value for the sector because the sector already has a 30-year history of protection. DHS Office of Infrastructure Protection officials acknowledged that these sectors have a long history of relationships with the federal government and in some cases have been doing similar planning efforts and said that while the NIPP planning process may not have been as valuable to these sectors, it was valuable to DHS to have plans for all critical infrastructure sectors. Representatives of 11 of 32 councils felt that the review process was too lengthy and said that they had turned in their plans in advance of the December 31, 2006, deadline established by the NIPP, but had to wait more than 5 months for the plans to be approved. DHS's Infrastructure Protection officials agreed that the review process had been lengthy and that time periods allowed for the sectors to respond to comments were too short. The officials said this occurred because of the volume of work DHS had to undertake and because some of the sector specific agencies did not communicate well with the sectors since they were still learning to operate effectively with the private sector, treating it as an equal partner under the NIPP model. The officials said that they plan to refine the process as the sector-specific agencies gain more experience working with the private sector. Conversely, representatives from eight of 32 councils said the review process for the plans worked well, despite the time it took, and five council representatives were complimentary of the support they received from DHS. The remaining council representatives did not offer views on these issues.

As we reported last year,[10] long-standing relationships were frequently cited as most helpful in establishing councils. Council representatives for 9 of the 32 councils continued to cite preexisting relationships as helping them in establishing and maintaining their sector councils, and two sectors noted that going through the process of establishing the councils had, in turn, improved relationships, while seven said achieving the necessary participation in the council is a continuing challenge. For example, the dams, energy, and banking and finance sectors, among others, said that existing relationships continue to help in maintaining their councils. On the other hand, seven sector council representatives reported difficulty in achieving and maintaining sector council membership, thus limiting the ability of the councils to effectively represent the sector. For example, the public health and health care sector representative said that getting sector members to participate is a challenge and noted that because of this, the first step in implementing the sector-specific plan is to increase awareness about the council. In addition, 11 of the 32 council representatives reported continuing difficulties with sharing information between the public and private sectors as a challenge. Furthermore, 6 of the 32 council representatives expressed concerns about the viability of the information system—the Homeland Security Information Network (HSIN)—DHS intends to rely on to share information with the sectors about critical infrastructure issues, as well as the effectiveness of the Protected Critical Infrastructure Information (PCII) program—a program that established procedures for the receipt, care, and storage of information submitted to DHS. Although encouraging the sectors to use HSIN, DHS's Infrastructure Protection officials said the system does not provide the capabilities that were promised, including providing the level of security expected by some sectors. Relatedly, in April 2007, we reported that the HSIN system was built without appropriate coordination with other information-sharing initiatives.[11] Additionally, as we have reported,[12] potential submitters under the PCII program continue to fear that the information, such as information on security vulnerabilities, could be inadequately protected,

[10]GAO, *Critical Infrastructure Protection: Progress Coordinating Government and Private Sector Efforts Varies by Sectors' Characteristics*, GAO-07-39 (Washington, D.C.: Oct. 16, 2006).

[11]GAO, *Information Technology: Numerous Federal Networks Used to Support Homeland Security Need to Be Better Coordinated with Key State and Local Information-Sharing Initiatives*, GAO-07-455 (Washington, D.C.: Apr. 16, 2007).

[12]GAO, *Information Sharing: DHS Should Take Steps to Encourage More Widespread Use of Its Program to Protect and Share Critical Infrastructure Information*, GAO-06-383 (Washington, D.C.: Apr. 17, 2006).

used for future legal or regulatory action, or inadvertently released. We previously recommended that, among other things, DHS better (1) define its critical infrastructure information needs and (2) explain how this information will be used to attract more users. DHS concurred with our recommendations. In September 2006, DHS issued a final rule that established procedures governing the receipt, validation, handling, storage, marking, and use of critical infrastructure information voluntarily submitted to DHS. DHS is in the process of implementing our additional recommendations that it better define its critical-infrastructure information needs under the PCII program and better explain how this information will be used to build the private sector's trust and attract more users.

Background

DHS serves as the sector-specific agency for 10 of the sectors: information technology; communications; transportation systems; chemical; emergency services; nuclear reactors, material, and waste; postal and shipping; dams; government facilities; and commercial facilities. Other sector-specific agencies are the departments of Agriculture, Defense, Energy, Health and Human Services, the Interior, the Treasury, and the Environmental Protection Agency. (See table 1 for a list of sector-specific agencies and a brief description of each sector).

Table 1: Designated Sector-Specific Agencies and Critical-Infrastructure Sectors

Sector-specific agency	Sector	Description
Departments of Agriculture,[a] and Health and Human Services, Food and Drug Administration[b]	Agriculture and food	Provides for the fundamental need for food. The infrastructure includes supply chains for feed and crop production. Carries out the postharvesting of the food supply, including processing and retail sales.
Department of Defense	Defense industrial base	Supplies the military with the means to protect the nation by producing weapons, aircraft, and ships and providing essential services, including information technology and supply and maintenance.
Department of Energy	Energy	Provides the electric power used by all sectors and the refining, storage, and distribution of oil and gas. The sector is divided into electricity and oil and natural gas.
Department of Health and Human Services	Public health and health care	Mitigates the risk of disasters and attacks and also provides recovery assistance if an attack occurs. The sector consists of health departments, clinics, and hospitals.
Department of the Interior	National monuments and icons	Memorializes or represents monuments, physical structures, objects, or geographical sites that are widely recognized to represent the nation's heritage, traditions, or values, or widely recognized to represent important national cultural, religious, historical, or political significance.
Department of the Treasury	Banking and finance	Provides the financial infrastructure of the nation. This sector consists of commercial banks, insurance companies, mutual funds, government-sponsored enterprises, pension funds, and other financial institutions that carry out transactions.
Environmental Protection Agency	Drinking water and water treatment systems	Provides sources of safe drinking water from more than 53,000 community water systems and properly treated wastewater from more than 16,000 publicly owned treatment works.
Department of Homeland Security:		
Office of Infrastructure Protection	Chemical	Transforms natural raw materials into commonly used products benefiting society's health, safety, and productivity. The chemical sector produces more than 70,000 products that are essential to automobiles, pharmaceuticals, food supply, electronics, water treatment, health, construction, and other necessities.
	Commercial facilities	Includes prominent commercial centers, office buildings, sports stadiums, theme parks, and other sites where large numbers of people congregate to pursue business activities, conduct personal commercial transactions, or enjoy recreational pastimes.
	Dams	Manages water retention structures, including levees, more than 77,000 conventional dams, navigation locks, canals (excluding channels), and similar structures, including larger and nationally symbolic dams that are major components of other critical infrastructures that provide electricity and water.
	Emergency services	Saves lives and property from accidents and disaster. This sector includes fire, rescue, emergency medical services, and law enforcement organizations.

Sector-specific agency	Sector	Description
	Nuclear reactors, materials, and waste	Provides nuclear power, which accounts for approximately 20 percent of the nation's electrical generating capacity. The sector includes commercial nuclear reactors and non-power nuclear reactors used for research, testing, and training; nuclear materials used in medical, industrial, and academic settings; nuclear fuel fabrication facilities; the decommissioning of reactors; and the transportation, storage, and disposal of nuclear materials and waste.
Office of Cyber Security and Communications	Information technology	Produces information technology and includes hardware manufacturers, software developers, and service providers, as well as the Internet as a key resource.
	Communications	Provides wired, wireless, and satellite communications to meet the needs of businesses and governments.
Transportation Security Administration	Postal and shipping	Delivers private and commercial letters, packages, and bulk assets. The U.S. Postal Service and other carriers provide the services of this sector.
Transportation Security Administration and U.S. Coast Guard	Transportation systems	Enables movement of people and assets that are vital to our economy, mobility, and security with the use of aviation, ships, rail, pipelines, highways, trucks, buses, and mass transit.
Immigration and Customs Enforcement, Federal Protective Service	Government facilities	Ensures continuity of functions for facilities owned and leased by the government, including all federal, state, territorial, local, and tribal government facilities located in the United States and abroad.

Source: NIPP, Homeland Security Presidential Directive 7, and the National Strategy for Homeland Security.

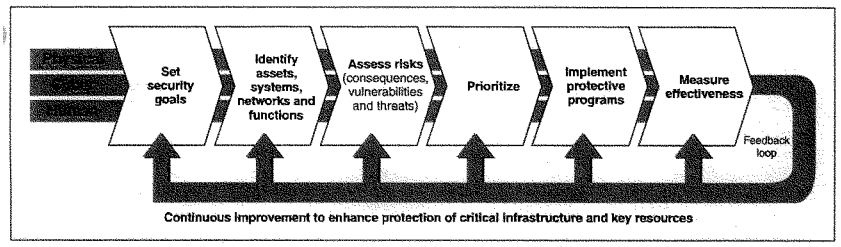
[a]The Department of Agriculture is responsible for food (including meat, poultry, and eggs) and agriculture.

[b]The Department of Health and Human Services, Food and Drug Administration, is responsible for food and other than meat, poultry, and egg products.

Most Sector Plans We Reviewed Met NIPP and DHS Sector-Specific Plan Guidance, but Varied Depending on Their Maturity and How They Define Their Assets

The nine sector-specific plans we reviewed generally met NIPP requirements and DHS's sector-specific plan guidance; however, the extent to which the plans met this guidance, and therefore their usefulness in enabling DHS to identify gaps and interdependencies across the sectors, varied depending on the maturity of the sector and on how the sector defines its assets, systems, and functions. As required by the NIPP risk management framework (see fig. 1), sector-specific plans are to promote the protection of physical, cyber, and human assets by focusing activities on efforts to (1) set security goals; (2) identify assets, systems, networks, and functions; (3) assess risk based on consequences, vulnerabilities, and threats;[13] (4) establish priorities based on risk assessments; (5) implement protective programs; and (6) measure effectiveness.

Figure 1: NIPP Risk Management Framework



Source: Department of Homeland Security: National Infrastructure Protection Plan.

In addition to these NIPP risk management plan elements outlined above and according to DHS's sector-specific plan guidance, the plans are also to address the sectors' efforts to (1) implement a research and development program for critical infrastructure protection and (2) establish a structure

[13]According to the NIPP, a "consequence" is the result of a terrorist attack or hazard that reflects the level, duration, and nature of the loss resulting from the incident. A "vulnerability" is a weakness in the design, implementation, or operation of an asset, system, or network that can be exploited by an adversary or disrupted by a natural hazard or technological failure. A "threat" is the intention and capability of an adversary to undertake actions that would be detrimental to critical infrastructure and key resources.

for managing and coordinating the responsibilities of the federal departments and agencies—otherwise known as sector-specific agencies—identified in HSPD-7 as responsible for critical-infrastructure protection activities specified for the 17 sectors.[14] Most of the plans included the required elements of the NIPP risk management framework, such as security goals and the methods the sectors expect to use to prioritize infrastructure, as well as to develop and implement protective programs. However, the plans varied in the extent to which they included key information required for each plan element. For example, all of the plans described the threat analyses that the sector conducts, but only one of the plans described any incentives used to encourage voluntary risk assessments, as required by the NIPP. Such incentives are important because a number of the industries in the sectors are privately owned and not regulated, and the government must rely on voluntary compliance with the NIPP. Additionally, although the NIPP called for each sector to identify key protective programs, three of the nine plans did not address this requirement. DHS officials told us that this variance in the plans can, in large part, be attributed to the levels of maturity and cultures of the sectors, with the more mature sectors generally having more comprehensive and complete plans than sectors without similar prior working relationships. For example, the banking and finance and energy sector plans included most of the key information required for each plan element. According to DHS officials, this is a result of these sectors having a history and culture of working with the government to plan and accomplish many of the same activities that are being required for the sector-specific plans. Therefore, these sectors were able to create plans that were more comprehensive and developed than those of less mature sectors, such as the public health and health care and agriculture and food sectors.

The plans also varied in how comprehensively they addressed their physical, human, and cyber assets, systems, and functions because sectors reported having differing views on the extent to which they were dependent on each of these assets, systems, and functions. According to DHS's sector-specific plan guidance, a comprehensive identification of such assets is important because it provides the foundation on which to conduct risk analysis and identify the appropriate mix of protective programs and actions that will most effectively reduce the risk to the nation's infrastructure. Yet, only one of the plans—drinking water and

[14]See appendix I for a full list of the requirements on which we evaluated the plans.

water treatment—specifically included all three categories of assets. For example, because the communications sector limited its definition of assets to networks, systems, and functions, it did not, as required by DHS's plan guidance, include human assets in its existing security projects and the gaps it needs to fill related to these assets to support the sector's goals. In addition, the national monuments and icons plan defined the sector as consisting of physical structures with minimal cyber and telecommunications assets because these assets are not sufficiently critical that damaging or destroying them would interfere with the continued operation of the physical assets. In contrast, the energy sector placed a greater emphasis on cyber attributes because it heavily depends on these cyber assets to monitor and control its energy systems. DHS officials also attributed the difference in the extent to which the plans addressed required elements to the manner in which the sectors define their assets and functions.

The plans, according to DHS's Office of Infrastructure Protection officials, are a first step in developing future protective measures. In addition, these officials said that the plans should not be considered to be reports of actual implementation of such measures. Given the disparity in the plans, it is unclear the extent to which DHS will be able to use them to identify gaps and interdependencies across the sectors in order to plan future protective measures. It is also unclear, from reviewing the plans, how far along each sector actually is in identifying assets, setting priorities, and protecting key assets. DHS officials said that to make this determination, they will need to review the sectors' annual progress reports, due in this month, that are to provide additional information on plan implementation as well as identify sector priorities.

Council Representatives Disagreed on the Value of the Plans and the Review Process

Representatives of 10 of 32 councils said the plans were valuable because they gave their sectors a common language and framework to bring the disparate members of the sector together to better collaborate as they move forward with protection efforts. For example, the government facilities council representative said that the plan was useful because relationships across the sector were established during its development that have resulted in bringing previously disjointed security efforts together in a coordinated way. The banking and finance sector's coordinating council representative said that the plan was a helpful way of documenting the history, the present state, and the future of the sector in a way that had not been done before and that the plan will be a working document to guide the sector in coordinating efforts. Similarly, an energy sector representative said that the plan provides a common format so that

all participants can speak a common language, thus enabling them to better collaborate on the overall security of the sector. The representative also said that the plan brought the issue of interdependencies between the energy sector and other sectors to light and provided a forum for the various sectors to collaborate. DHS's Office of Infrastructure Protection officials agreed that the main benefit of these plans was that the process of developing them helped the sectors to establish relationships between the private sector and the government and among private sector stakeholders that are key to the success of protection efforts.

However, representatives of 8 of the 32 councils said the plans were not useful to their sectors because (1) the plans did not represent a true partnership between the federal and private sectors or were not meaningful to all the industries represented by the sector or (2) the sector had already taken significant protection actions, thus, developing the plan did not add value. The remaining council representatives did not offer views on this issue. Sector representatives for three transportation modes—rail, maritime, and aviation—reported that their sector's plan was written by the government and that the private sector did not participate fully in the development of the plan or the review process. As a result, the representatives did not believe that the plan was of value to the transportation sector as a whole because it does not represent the interests of the private sector. Similarly, agriculture and food representatives said writing the plan proved to be difficult because of the sector's diversity and size—more than 2,000,000 farms, one million restaurants, and 150,000 meat processing plants. They said that one of the sector's biggest challenges was developing a meaningful document that could be used by all of the industries represented. As a result of these challenges, the sector submitted two plans in December 2006 that represented a best effort at the time, but the sector council said it intends to use the remainder of the 2007 calendar year to create a single plan that better represents the sector. In contrast, the coordinating council representative for nuclear reactors, materials, and waste sector said that because the sector's security has been robust for a long time, the plan only casts the security of the sector in a different light, and the drinking water and water treatment systems sector said that the plan is a "snapshot in time" document for a sector that already has a 30-year history of protection, and thus the plan did not provide added value for the sector. Officials at DHS's Office of Infrastructure Protection acknowledged that these sectors have a long history of working together and in some cases have been doing similar planning efforts. However, the officials said that the effort was of value to the government because it now has plans for all

17 sectors and it can begin to use the plans to address the NIPP risk management framework.

Representatives of 11 of 32 councils said the review process associated with the plans was lengthy. They commented that they had submitted their plans in advance of the December 31, 2006, deadline, but had to wait 5 months for the plan to be approved. Eight of them also commented that while they were required to respond within several days to comments from DHS on the draft plans, they had to wait relatively much longer during the continuing review process for the next iteration of the draft. For example, a representative of the drinking water and water treatment sector said that the time the sector had to incorporate DHS's comments into a draft of the plan was too short—a few days—and this led the sector to question whether its members were valued partners to DHS. DHS's Infrastructure Protection officials agreed that the review process had been lengthy and that the comment periods given to sector officials were too short. DHS officials said this occurred because of the volume of work DHS had to undertake and because some of the sector-specific agencies were still learning to operate effectively with the private sector under a partnership model in which the private sector is an equal partner. The officials said that they plan to refine the process as the sector-specific agencies gain more experience working with the private sector.

Conversely, representatives from eight of 32 councils said the review process for the plans worked well, and five of these council representatives were complimentary of the support they received from DHS. The remaining council representatives did not offer views on this topic. For example, an information technology (IT) sector coordinating council representative said that the review and feedback process on their plan worked well and that the Office of Infrastructure Protection has helped tremendously in bringing the plans to fruition. However, sector coordinating council representatives for six sectors also voiced concern that the trusted relationships established between the sectors and DHS might not continue if there were additional turnover in DHS, as has occurred in the past. For example, the representative of one council said they had established productive working relationships with officials in the Offices of Infrastructure Protection and Cyber Security and Communications, but were concerned that these relationships were dependent on the individuals in these positions and that the relationships may not continue without the same individuals in charge at DHS. As we

have reported in the past, developing trusted partnerships between the federal government and the private sector is critical to ensure the protection of critical infrastructure.[15]

Long-standing Relationships Continue to Facilitate Councils, but Some Council Representatives Reported Information-Sharing Challenges

Nine of 32 sector representatives said that their preexisting relationships with stakeholders helped in establishing and maintaining their sector councils, and two noted that establishing the councils had improved relationships. Such participation is critical to well-functioning councils. For example, representatives from the dams, energy, and banking and finance sectors, among others, said that existing relationships continue to help in maintaining their councils. In addition, the defense industrial base representatives said the organizational infrastructure provided by the sector councils is valuable because it allows for collaboration. Representatives from the national monuments and icons sector said that establishing the government sector council has facilitated communication within the sector. We also reported previously that long-standing relationships were a facilitating factor in council formation and that 10 sectors had formed either a government council or sector council that addressed critical infrastructure protection issues prior to DHS's development of the NIPP.[16] As a result, these 10 sectors were more easily able to establish government coordinating councils and sector coordinating councils under the NIPP model. Several councils also noted that the Critical Infrastructure Partnership Advisory Council (CIPAC), created by DHS in March 2006 to facilitate communication and information sharing between the government and the private sector, has helped facilitate collaboration because it allows the government and industry to interact without being open to public scrutiny under the Federal Advisory Committee Act.[17] This is important because previously,

[15]GAO, *Critical Infrastructure Protection: Improving Information Sharing with Infrastructure Sectors*, GAO-04-780 (Washington, D.C.: July 9, 2004) and *Information Sharing: Practices That Can Benefit Critical Infrastructure Protection*, GAO-02-24 (Washington, D.C.: Oct. 15, 2001).

[16]See GAO-07-39.

[17]The Federal Advisory Committee Act (codified at 5 U.S.C. app. 2) was enacted, in part, to control the advisory committee process and to open to public scrutiny the manner in which government agencies obtain advice from private individuals and groups. See 648 F. Supp. 1353, 1358-59 (D.D.C. 1986). Section 871 of the Homeland Security Act authorized a process under which the Secretary could exempt an advisory committee from the Federal Advisory Committee Act. See Pub. L. No. 107-296, § 871, 116 Stat. 2135, 2243.

meetings between the private sector and the government had to be open to the public, hampering the private sector's willingness to share information.

Conversely, seven sector council representatives reported difficulty in achieving and maintaining sector council membership, thus limiting the ability of the councils to effectively represent the sector. For example, the public health and health care sector representative said that getting the numerous sector members to participate is a challenge, and the government representative noted that because of this, the first step in implementing the sector-specific plan is to increase awareness about the effort among sector members to encourage participation. Similarly, due to the size of the commercial facilities sector, participation, while critical, varies among its industries, according to the government council representative. Meanwhile, the banking and finance sector representatives said that the time commitment for private sector members and council leaders makes participation difficult for smaller stakeholders, but getting them involved is critical to an effective partnership. Likewise, the IT sector representatives said engaging some government members in joint council meetings is a continuing challenge because of the members' competing responsibilities. Without such involvement, the officials said, it is difficult to convince the private sector representatives of the value of spending their time participating on the council.

Additionally, obtaining state and local government participation in government sector councils remains a challenge for five sectors. Achieving such participation is critical because these officials are often the first responders in case of an incident. Several government council representatives said that a lack of funding for representatives from these entities to travel to key meetings has limited state and local government participation. Others stated that determining which officials to include was a challenge because of the sheer volume of state and local stakeholders. DHS Infrastructure Protection officials said that the agency is trying to address this issue by providing funding for state and local participation in quarterly sector council meetings and has created a State, Local and Tribal and Territorial Government Coordinating Council (SLTTGCC)—composed of state, local, tribal, and territorial homeland security advisers—that serves as a forum for coordination across these jurisdictions on protection guidance, strategies, and programs.

Eleven of the 32 council representatives reported continuing challenges with sharing information between the federal government and the private sector. For example, six council representatives expressed concerns about the viability of two of DHS's main information-sharing tools—the

Homeland Security Information Network (HSIN) or the Protected Critical Infrastructure Information (PCII) program. We reported in April 2007 that the HSIN system was built without appropriate coordination with other information-sharing initiatives.[18] In addition, in a strategic review of HSIN, DHS reported in April 2007 that it has not clearly defined the purpose and scope of HSIN and that HSIN has been developed without sufficient planning and program management. According to DHS Infrastructure Protection officials, although they encouraged the sectors to use HSIN, the system does not provide the capabilities that were promised, including providing the level of security expected by some sectors. As a result, they said the Office of Infrastructure Protection is exploring an alternative that would better meet the needs of the sectors. In addition, three council representatives expressed concerns about whether information shared under the PCII program would be protected. Although this program was specifically designed to establish procedures for the receipt, care, and storage of critical infrastructure information submitted voluntarily to the government, the representatives said potential submitters continue to fear that the information could be inadequately protected, used for future legal or regulatory action, or inadvertently released.

In April 2006, we reported that DHS faced challenges implementing the program, including being able to assure the private sector that submitted information will be protected and specifying who will be authorized to have access to the information, as well as to demonstrate to the critical infrastructure owners the benefits of sharing the information to encourage program participation.[19] We recommended, among other things, that DHS better (1) define its critical-infrastructure information needs and (2) explain how this information will be used to attract more users. DHS concurred with our recommendations. In September 2006 DHS issued a final rule that established procedures governing the receipt, validation, handling, storage, marking, and use of critical infrastructure information voluntarily submitted to DHS. DHS is in the process of implementing our additional recommendations that it define its critical-infrastructure information needs under the PCII program and better explain how this information will be used to build the private sector's trust and attract more users.

[18]See GAO-07-455.

[19]See GAO-06-383.

Concluding Observations

To date, DHS has issued a national plan aimed at providing a consistent approach to critical infrastructure protection, ensured that all 17 sectors have organized to collaborate on protection efforts, and worked with government and private sector partners to complete all 17 sector-specific plans. Nevertheless, our work has shown that sectors vary in terms of how complete and comprehensive their plans are. Furthermore, DHS recognizes that the sectors, their councils, and their plans must continue to evolve. As they do and as the plans are updated and annual implementation reports are provided that begin to show the level of protection achieved, it will be important that the plans and reports add value, both to the sectors themselves and to the government as a whole. This is critical because DHS is dependent on these plans and reports to meet its mandate to evaluate whether gaps exist in the protection of the nation's most critical infrastructure and key resources and, if gaps exist, to work with the sectors to address the gaps. Likewise, DHS must depend on the private sector to voluntarily put protective measures in place for many assets. It will also be important that sector councils have representative members and that the sector-specific agencies have buy-in from these members on protection plans and implementation steps. One step DHS could take to implement our past recommendations to strengthen the sharing of information is for the PCII program to better define its critical infrastructure information needs and better explain how this information will be used to build the private sector's trust and attract more users. As we have previously reported, such sharing of information and the building of trusted relationships are crucial to the protection of the nation's critical infrastructure.

Mr. Chairman, this concludes my statement. I would be pleased to answer any questions that you or other members of the subcommittee may have at any time.

Contact Information

For further information on this testimony, please contact Eileen Larence at (202) 512-8777 or by e-mail at larencee@gao.gov. Individuals making key contributions to this testimony include Susan Quinlan, Assistant Director; R. E. Canjar; Landis Lindsey; E. Jerry Seigler; and Edith Sohna.

Appendix I: Criteria Used to Determine Completeness of Sector Specific Plans

We assessed the sector specific plans (SSPs) using 8 criteria, consisting of 40 key information requirements. We extracted this information from the requirements included in the NIPP as well as on the detailed sector-specific plan guidance issued by DHS. Each criterion reflects a component DHS required for the completion of the SSP. The 8 criteria we used are listed below along with the corresponding 40 key information requirements.

Section 1: Sector Profile and Goals

1. Did the sector include physical and human assets as part of its sector profile?[1]

2. Does the SSP identify any regulations or key authorities relevant to the sector that affect physical and human assets and protection?

3. Does the SSP show the relationships between the sector specific agency and the private sector, other federal departments and agencies, and state and local agencies that are either owner/operators of assets or provide a supporting role to securing key resources?

4. Does the SSP contain sector-specific goals?

5. Does the SSP communicate the value of the plan to the private sector, other owners, and operators?

Section 2: Identify Assets, Systems, Networks, and Functions

6. Does the SSP include a process for identifying the sector's assets and functions, both now and in the future?

7. Does the SSP include a process to identify physical and human asset dependencies and interdependencies?

8. Does the SSP describe the criteria being used to determine which assets, systems, and networks are and are not of potential concern?

9. Does the SSP describe how the infrastructure information being collected will be verified for accuracy and completeness?

[1]A companion engagement assessed the plans for inclusion of cyber assets.

Section 3: Assess Risks

10. Does the SSP discuss the risk assessment process, including whether the sector is mandated by regulation or are primarily voluntary in nature.

11. Does the SSP address whether a screening process (process to determine whether a full assessment is required) for assets would be beneficial for the sector, and if so, does it discuss the methodologies or tools that would be used to do so?

12. Does the SSP identify how potential consequences of incidents, including worst case scenarios, would be assessed?

13. Does the SSP describe the relevant processes and methodologies used to perform vulnerability assessments?

14. Does the SSP describe any threat analyses that the sector conducts?

15. Does the SSP describe any incentives used to encourage voluntary performance of risk assessments?

Section 4: Prioritize Infrastructure

16. Does the SSP identify the party responsible for conducting a risk-based prioritizing of the assets?

17. Does the SSP describe the process, current criteria, and frequency for prioritizing sector assets?

18. Does the SSP provide a common methodology for comparing both physical and human assets when prioritizing a sector's infrastructure?

Section 5: Develop and Implement Protective Programs

19. Does the SSP describe the process that the SSA will use to work with asset owners to develop effective long-term protective plans for the sector's assets?

20. Does the SSP identify key protective programs (and their role) in the sector's overall risk management approach?

21. Does the SSP describe the process used to identify and validate specific program needs?

22. Does the SSP include the minimum requirements necessary for the sector to prevent, protect, respond to, and recover from an attack?

23. Does the SSP address implementation and maintenance of protective programs for assets once they are prioritized?

24. Does the SSP address how the performance of protective programs is monitored by the sector-specific agencies and security partners to determine their effectiveness?

Section 6: Measure Progress

25. Does the SSP explain how the SSA will collect, verify and report the information necessary to measure progress in critical infrastructure/key resources protection?

26. Does the SSP describe how the SSA will report the results of its performance assessments to the Secretary of Homeland Security?

27. Does the SSP call for the development and use of metrics that will allow the SSA to measure the results of activities related to assets?

28. Does the SPP describe how performance metrics will be used to guide future decisions on projects?

29. Does the SSP list relevant sector-level implementation actions that the SSA and its security partners deem appropriate?

Section 7: Research and Development for Critical Infrastructure/Key Resources Protection

30. Does the SSP describe how technology development is related to the sector's goals?

31. Does the SSP identify those sector capability requirements that can be supported by technology development?

32. Does the SSP describe the process used to identify physical and human sector-related research requirements?

33. Does the SSP identify existing security projects and the gaps it needs to fill to support the sector's goals?

34. Does the SSP identify which sector governance structures will be responsible for R&D?

35. Does the SSP describe the criteria that are used to select new and existing initiatives?

Section 8: Manage and Coordinate SSA Responsibilities

36. Does the SSP describe how the SSA intends to staff and manage its NIPP responsibilities? (e.g., creation of a program management office.)

37. Does the SSP describe the processes and responsibilities of updating, reporting, budgeting, and training?

38. Does the SSP describe the sector's coordinating mechanisms and structures?

39. Does the SSP describe the process for developing the sector-specific investment priorities and requirements for critical infrastructure/key resource protection?

40. Does the SSP describe the process for information sharing and protection?

PRIVATE-SECTOR PREPAREDNESS

IN CRITICAL INFRASTRUCTURE PROTECTION

Testimony of
Kenneth C. Watson
Vice Chairman, Partnership for Critical Infrastructure Security, Inc. (PCIS)

To
U.S. Senate
Senate Homeland Security and Government Affairs Committee
Ad Hoc Committee on State, Local and Private Sector Preparedness and Integration

Washington, D.C.
July 12, 2007

Mr. Chairman and Members of the Subcommittee:

I am Ken Watson, Manager of Cisco's Critical Infrastructure Assurance Group. I am here today in my capacity as the elected Vice Chairman of the Partnership for Critical Infrastructure Security (PCIS). Thank you for inviting the PCIS to participate in today's hearing on America's private-sector preparedness to protect our critical infrastructure. I believe the nation's critical infrastructures and key resources represent the new "center of gravity" for defending our national and economic security. The companies and associations that constitute the membership of PCIS are eager to continue doing their part to ensure the ongoing delivery of critical infrastructure services on which the nation and its citizens depend for just about everything we do, day in and day out.

The increasingly interconnected nature of the world's economy has created a global marketplace of ideas and commerce. Every industry in the United States, and throughout the developed world, is increasingly dependent on every other. The Federal government relies on the services provided by private-sector infrastructure owners and operators. Many of these owners and operators lead multinational corporations, and all have an interlaced global network of suppliers, partners, and customers. The health of this networked global economy is directly relevant to the health of America's national and economic security.

The National Infrastructure Protection Plan (NIPP) designates the PCIS as the private-sector cross-sector coordinating council for protecting critical infrastructure. Our council consists of the Sector Coordinating Councils (SCCs) for all the critical infrastructure sectors designated in Homeland Security Presidential Directive-7 (HSPD-7) that have private-sector components. (The Government Facilities and National Monuments and Icons sectors do not have private-sector components). The strength of the PCIS is generated by the expertise and leadership found in those SCCs. In turn, SCCs reflect the make-up of the key companies and leaders in the sectors. Most of the sectors have also established Information Sharing and Analysis Centers (ISACs) to manage their day-to-day information sharing needs. As I discuss progress and perspectives of the sectors, I will underscore the roles of the SCCs and the ISACs.

In response to a call for public-private partnership from the Federal government, several private-sector critical infrastructure owners and operators founded PCIS in 1999. That call was itself a response to the October 1997 report of the President's Commission on Critical Infrastructure Protection (PCCIP), "Critical Foundations," led by retired General Robert Marsh. Because of what it characterized as two irreversible trends, the Marsh Commission found that a strong public-private partnership was the only path to secure infrastructures. Those two trends—increasing privatization of critical services and increasing migration of core business and government operations to networks, including the Internet—continue today. Government can no longer defend the country by itself—it has neither the specialized expertise nor the network access required.

The private sector has not organized itself neatly into departments and agencies as the government has. Therefore, there were unique challenges in constructing an architecture that not only reached the right expertise in each sector, but also provided for universal access for all sector members. Moreover, the framework would need to include a robust, multi-level information-sharing mechanism that could reach executives and experts in a timely manner. Not

surprisingly, the first attempts at building this partnership had mixed success—on both the public and private-sector sides of the partnership. Nevertheless, after eight years of hard work, we have made tremendous progress. It is not perfect, but I believe we are on a very solid path, and the United States is far more resilient to potential attacks or natural disasters affecting critical infrastructures than it was eight years ago.

Today, I will provide an overview of PCIS goals, present examples of recent progress, offer benchmarks for continued success, address some specific concerns and perspectives of the sectors, and discuss joint industry-DHS initiatives to remove barriers to private-sector participation in the partnership. Finally, I will offer suggestions regarding what the government might do to continue strengthening this partnership and improving our resilience in both physical and cyber security.

When we created PCIS, we envisioned it as a cross-sector coordination mechanism for policy and strategy matters, neither operational nor authoritative in its own right. SCCs are the resident experts from the sectors, and therefore we defer to that expertise for specific questions regarding sector operations. The PCIS mission is to "coordinate cross-sector initiatives that promote public and private efforts to ensure secure, safe, and reliable critical infrastructure services." This overall goal continues today. This past April, we published our first comprehensive business plan, which covers the three-year period 2007 to 2009. I have attached it to my written testimony for your reference.

The business plan outlines PCIS objectives, products and services, strategies for communications, organization, management, operations, research and development, and support, and it provides details on our current working groups and committees. Our members tell us they see value in understanding issues common to multiple sectors, unique challenges or solutions from a single sector, and the ability to jointly approach DHS and other government organizations.

Primarily, PCIS seeks to improve continuously the overall national capability to ensure critical infrastructure services and protect supporting critical assets and functions. We accomplish our mission by fulfilling the following roles:

- Address physical, cyber, and human cross-sector critical infrastructure protection and interdependency issues of concern to sector owners and operators;
- Improve the security and safety of the nation's critical infrastructures by enabling critical infrastructure sectors to collaborate among themselves, as well as in partnership with governments;
- Encourage and participate in productive public-private partnerships with government as enabled by the Critical Infrastructure Partnership Advisory Council (CIPAC);
- Participate in CIPAC (through PCIS members); and
- Serve as the Private-Sector Cross-Sector Council in the NIPP Sector Partnership Framework.

PCIS is guided by three core principles:

1. *Build effective collaborative relationships between the sectors and government by improving coordination, cooperation and communication.*
2. *Promote a comprehensive approach to detect, prepare, prevent, protect, respond and recover from all threats and hazards that may cause incidents of national significance.*
3. *Promote the merits of a non-regulatory approach to advance the security and resilience of the sectors.*

The PCIS business plan identifies four broad goals, each with subordinate objectives and metrics.

1. Partnership Leadership for all-sector critical infrastructure protection issues and policy;
2. Cross-Sector Leadership for cross-sector and interdependency issues;
3. Sector Assistance for healthy and productive partnership interactions; and
4. PCIS Effectiveness for strong organizational effectiveness and value.

In addition, because of the comprehensive, sector-specific subject-matter expertise resident in PCIS, the National Infrastructure Advisory Council (NIAC) calls on us from time to time as it develops policy advice for the President. Two notable recent efforts were:

- Prioritization of Critical Infrastructure for a Pandemic Outbreak in the United States; and
- Public-Private Sector Intelligence Coordination.

There are numerous examples of recent successes. Chief among those is development of the NIPP and its 17 Sector-Specific Plans (SSPs). The level of collaboration we enjoyed would have been impossible without the CIPAC framework provided by the Congress in the Homeland Security Act of 2002 and implemented by Secretary Chertoff more than a year ago. CIPAC represents a partnership between government and critical infrastructure/key resource (CI/KR) owners and operators. The Council provides a forum in which these partners can engage, freely and openly, in a broad spectrum of activities to support and coordinate critical infrastructure protection. The CIPAC framework allowed us to roll up our sleeves and work side-by-side with our government counterparts to write these plans.

One significant result of this collaboration is the NIPP's approach to risk management. Before private-sector participation began, the draft proposed a bottom-up approach, which focused on physical assets. But after considerable engagement between DHS and sectors that are less dependent on specific physical assets than on functional systems (such as electric power, communications, and information technology), the NIPP risk management section evolved to accommodate top-down, functionally-based risk management models, permitting these multiple approaches.

The incorporation of the top-down, functional approach reshaped the NIPP into a useful framework for all the SSPs, not just for those with a finite number of discrete physical assets. Rather than using taxpayer funds to develop border-zone protections for these sectors, the NIPP framework will eventually identify smarter ways to spend Federal resources. One example of a sector with a top-down, functional approach can be found in the Communications Sector.

- Communications—Communications networks are dynamic; the most important assets change depending on the circumstances. Some of the most important assets may be the people assigned by companies to the National Coordinating Center for Telecommunications. They work with each other under mutual support agreements, coordinating closely with 23 Federal agencies on day-to-day incidents, including everything from backhoe cable cuts to Denial of Service (DoS) attacks against carriers.

Developing the SSPs was not a perfect process. Not all Sector-Specific Agencies (SSAs) worked as closely with their private-sector counterparts as others. Most sectors were very pleased with their collaboration, but for others a learning curve remains. I see these as growing pains as both government and owner-operators embrace the new partnership framework.

I am happy to report the list of sector successes is a long one, and growing by the day. So now, I would like to mention six success stories, each one of which is representative of the tremendous work and progress all of our critical infrastructure sectors are making.

- Financial Services—In 2003, 14 Chicago-area financial institutions formed a nonprofit organization called ChicagoFIRST, which they designed to address homeland security and emergency management issues requiring a coordinated response with all levels of government. Today, ChicagoFIRST is 26 members strong, and growing. The group collaborates daily with the City of Chicago, State of Illinois, and numerous Federal agencies on disaster management matters. Since it was founded, ChicagoFIRST has obtained a seat in the Chicago emergency operations center for the financial community, encouraged the city to implement a credentialing system, assisted in planning and executing an evacuation of four downtown skyscrapers, ensured that members receive important emergency information from government, and worked with the city and State on pandemic preparedness. Now, similar regional partnerships are forming, using ChicagoFIRST as a model. A new informal organization, RPC FIRST (Regional Partnership Council for Financial Industry Resilience, Security, and Teamwork) shares best practices, solicits advice, and participates in the national Financial Services Sector Coordinating Council (FSSCC).
- Rail and Water—The Association of American Railroads (AAR) is working with three ISACs, which meet quarterly with intelligence personnel from DHS, FBI, CIA, National Security Agency, and the Middle Atlantic-Great Lakes Organized Crime Law Enforcement Network to add realism and usefulness to quarterly industry threat assessments. These meetings have enhanced mutual trust, increased knowledge of cross-sector dependencies, and raised understanding among government analysts of rail industry operational characteristics. In addition, the WaterISAC, managed by the Association of Metropolitan Water Agencies, also conducts quarterly meetings with intelligence personnel from DHS, FBI, and others to crosscheck the Sector's intelligence gathering efforts with those of the Federal intelligence community.
- Dams—In addition to holding classified briefings and establishing a Dams portal on the Homeland Security Information Network (HSIN), the Dams Sector has developed a close working relationship with the DHS National Cyber Security Division (NCSD). The Dams Sector assists DHS and the Federal Energy Regulatory Commission (FERC) conduct annual security seminars for the FERC-regulated Sector members. To educate owners of smaller dams about current and future security initiatives as well as assessments of threats, the Dams Sector draws on the expertise of various member associations.

- Water—The American Water Works Association (AWWA), with support from the Environmental Protection Agency (EPA) and other Sector associations, has been leading an initiative to support the development of intrastate mutual aid and assistance networks between water and wastewater utilities (public and private) to increase the Sector's preparedness and response capability to natural and man-made incidents. For the past year, the Sector has put on workshops to introduce the concept and develop action plans. Currently there are nine Water/Wastewater Agency Response Network (WARN) states, and more than 30 states are currently establishing a WARN program.
- Commercial Facilities—The International Association of Assembly Managers (IAAM) used a DHS Competitive Training Grant to create a six-hour training course to assist in promoting and training facility managers on the Vulnerability Identification Self-Assessment Tool (ViSAT). DHS developed ViSAT, a Web-based tool, to enable asset owners and operators to provide security awareness training and to conduct voluntary vulnerability assessments of their facilities. Within the Commercial Facilities Sector, modules have been programmed into the system for stadiums, arenas, performing arts centers, and convention centers. IAAM has identified between 12 and 15 locations in the public assembly community to roll out the ViSAT training program.
- Nuclear—The Nuclear Sector represents all 104 operating U.S. nuclear power reactors, research and test reactors, and the radioisotope community. It formed in late 2004, and, in a short period, worked collaboratively with DHS to develop and implement the Risk Analysis and Management for Critical Asset Protection (RAMCAP) and Comprehensive Review (CR) processes. By the end of this year, RAMCAPs and CRs will be completed at all operating nuclear power reactors in the United States. Most importantly, insights from CRs have led to actions taken by plant owners and emergency responders (Federal, State, and local) that have made significant improvements to the security posture and responsive capabilities for those key resources. Further, with DHS, the Nuclear Sector completed initial planning for pandemic flu preparedness by early 2006, and has advanced that effort within the Sector and worked outside the Nuclear Sector to help more broadly. Moreover, in several specific intelligence and technical areas, the Sector has worked very closely with the Department of Homeland Security (DHS) in a manner that has led to measurable improvement in the security of our nuclear power plants.

Removing any perceived or actual barriers to private-sector participation is a key initiative of DHS, as well as the PCIS. In your invitation, the Subcommittee asked me to comment on three areas of concern today:

1. Issues of competitive advantage;
2. Fear of sharing sensitive information; and
3. Worries the partnership might exclude smaller operators.

Regarding competition, a quote by Gregg Jones in a recent Business Executives for National Security (BENS) report, "Getting Down To Business," reflects the way PCIS operates. "We're competitors, not enemies," wrote Jones, the Chief Administrative Officer for Greenberg Traurig, LLP. "We collaborate during emergencies..." The same holds true for the SCCs and ISACs. I have seen this collaborative approach across all the sectors from the creation of PCIS through today, and I assure you these efforts are not merely about marketing or selling to customers.

Business works with our government partners to develop policies, strategies, and information-sharing mechanisms we will all rely on during an emergency. ISACs, and their relationship to DHS, provide an excellent example of these non-competitive partnerships in action. Sectors that have ISACs use them to share information on threats, vulnerabilities, countermeasures, and best practices. ISACs coordinate regularly with each other and with the DHS U.S. Computer Emergency Readiness Team (US-CERT). PCIS is leveraging the ISAC Council (an *ad-hoc* coalition of the leadership of most of the industry ISACs) as it works with DHS on information-sharing policy issues.

Regarding sharing sensitive information, we are working closely with the Protected Critical Infrastructure Information (PCII) Program Office and the Information Sharing Environment (ISE) on two initiatives that would improve information sharing while also protecting sensitive information. The President tasked the ISE to reform the classification criteria for "Sensitive But Unclassified" (SBU) information. Under the CIPAC framework, PCIS members are working with ISE and DHS personnel to develop a simplified, rational approach to protecting information. Most recently, the ISE combined our latest comments with those of Federal departments and agencies in a draft guideline document that is on its way to a Principals Committee review. As long as statutory protections (for CII) remain in place, the PCII program should function within the newly proposed "Controlled Unclassified Information" (CUI) environment. Despite these efforts, some sectors continue to have serious concerns for two primary reasons. First, sectors are unclear about what sensitive information DHS needs. Second, sectors remain concerned this information may be disclosed publicly, making it available to competitors or used in litigation.

In regards to including smaller operators, sectors have organized their SCCs to include all relevant trade and operational associations. This was a provision the private sector insisted upon, and DHS agreed to incorporate into CIPAC. An example of inclusion is the Food and Agriculture SCC, which has 119 separate entities representing all aspects of the Sector from "farm to table," including restaurants, grocery stores, meat packers, farmers, and food processors. Another is the Financial Services SCC, which has 34 associations and companies, representing banks, brokerages, and the insurance industry. Each SCC is aggressively pursuing ways to increase its reach, and I believe most of them are growing accordingly. In addition, Assistant Secretary Bob Stephan and others from DHS regularly travel around the country, conducting town hall-style meetings, where officials encourage companies and associations to join SCCs and ISACs.

Finally, please allow the PCIS to make a few suggestions our members feel would not only enhance the existing partnership but also improve our country's ability to manage exceptional events.

First, let the partnership mature. It is working, but it's still young. We have accomplished a great deal with DHS since its inception and adoption of the PCIS as the framework for private-sector engagement, and even more in the year since Secretary Chertoff exercised the Section 871 exemption and created CIPAC. We are still exploring ways to use that framework.

We welcome the involvement of Congress, but we need to continue a trusted environment in order to work with our government partners on sensitive issues affecting our safety and security.

We would be happy to work with you as you consider standards and risk assessments so we can build on the trust we have established and capitalize on the free flow of ideas and solutions we are beginning to enjoy under the new framework.

Second, help us educate all Federal departments and agencies regarding the nature of this partnership. The partnership model is a good one, but not uniformly executed across the sectors. This is due, in part, to the need of some in the Federal government to be educated on the value of the partnership model. Many we work with in DHS' operating group for IT and communications and the Department's Partnership and Outreach Division understand the structure, but the further one gets away from those offices, the less understanding and appreciation of the Sector Partnership Framework there is.

We also need help internationally. The public-private partnership is the right model globally, and as other countries grapple with these same issues, the U.S. government can continue to lead, and even increase, global education efforts touting the benefits of public-private partnerships, and the primacy of ensuring innovation and flexibility in the critical infrastructure discipline.

Third, we must reform the National Response Plan (NRP) process to reflect the true partnership model we have found with the development of the NIPP. Additionally, the NRP text and annexes should be reviewed to include more private-sector participation early in response actions. This is important when dealing with physical incidents, but even more important when you consider the cyber dimension. Critical infrastructure owners and operators understand their interdependencies, especially on the global arena. PCIS considers all cyber incidents international by default. The private sector already has multiple collaborative mechanisms in place to deal with significant cyber incidents. Many Internet Service Providers (ISPs) collaborate through the informal "nsp-sec" community. Multiple government and private-sector incident response teams belong to the more formal Forum of Incident Response and Security Teams (FIRST). These two global organizations respond in real time, and we should begin thinking of them as "global cyber first responders." The NRP should incorporate turning to these organizations, and other private-sector organizations like them, for any cyber incident of national significance.

Fourth and finally, the government must share more timely and useful information with the private sector. It is often difficult to determine exactly who "needs to know" sensitive information, but the Sector Partnership Framework includes enough trust to err on the "need to share" side of the equation. Complex interdependencies, a lack of familiarity with sector operations, and little-known collocation of assets argue for the sharing of alerts and warnings with PCIS and relevant ISACs rather than trying to ferret out only those owners and operators that government analysts think might be involved in an incident. Many of the ISACs are capable of transmitting and storing classified material, and many sectors have cleared individuals that can be trusted with sensitive information. The Emergency Notification System (ENS), for example, has worked well on the few occasions DHS has used it. DHS has done a relatively good job establishing it, though it the Department could exercise it more frequently and should update it regularly with a PCIS list, ISAC list, and other key executives, as required.

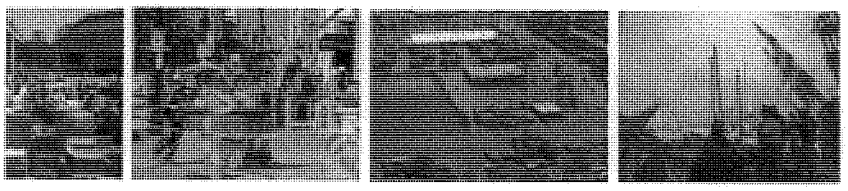
Thank you again for the opportunity to be with you today on behalf of PCIS. Now I would be happy to answer any questions you have.

Executives
National Security

Getting Down to Business:

An Action Plan for Public-Private Disaster Response Coordination

The Report of the Business Response Task Force



January 2007

Table of Contents

Preface 2

Key Findings and Recommendations 4

Introduction: Background, Methods and Aims 6

Chapter 1. Public-Private Collaboration 13

Chapter 2. Surge Capacity/Supply Chain Management 21

Chapter 3. Legal & Regulatory Environment 31

Chapter 4. An Expert's Guide to Priorities and Sequencing for the Integration of the Private Sector into U.S. National Disaster Response Planning and Execution 36

Appendices

A - Business Response Task Force Charter 41

B - Task Force Members, Advisors and Staff 42

C - List of Survey Interviews 44

D - Relevant Recommendations from Federal Government After-action Reports and Other Sources 46

E - Glossary of Acronyms in this Report 50

F - Public-Private Collaboration Outcomes and Drivers 54

G - Surge Capacity/Supply Chain Management Outcomes and Drivers 55

H - Legal & Regulatory Environment Outcomes and Drivers 57

I - Priorities and Sequencing Outcomes and Drivers 58

Preface

The 2005 hurricane season and its prolonged crisis aftermath demonstrated beyond doubt that the United States is not adequately prepared to deal with major catastrophes, whether natural or man-made. Coming nearly four years after the 9/11 attacks, the inadequate local, state and federal government responses to Hurricane Katrina put the entire nation on alert that America has many problems to overcome before being truly ready to mount a reinforced and efficient disaster response.

Not least of these problems is the systematic failure of government to integrate the resources of America's vast private sector into its disaster response plans, up to and including response to an Incident of National Significance.[1] As the February 26, 2006, White House report, *The Federal Response to Hurricane Katrina: Lessons Learned*, stated:

> *The Federal government should recognize that the private/non-government sectors often perform certain functions more efficiently and effectively than government because of the expertise and experience in applying successful business models. These public-private partnerships should be facilitated, recognized, funded [and]. . . the capability to draw on these resources should inform and be part of Federal, State, and local logistics systems and response plans.*

Invited by the senior leadership of both the United States Senate and U.S. House of Representatives to offer advice, in June 2006 Business Executives for National Security (BENS) formed a Task Force to recommend to the U.S. Government steps to systematically integrate the capabilities of the private sector—principally those of the business community—into a comprehensive national disaster response mechanism.

BENS did so in response not only to the federal government's recognition of a pressing need in the aftermath of Katrina, but also in response to the overwhelming demand of its membership. During the summer and autumn of 2005, many BENS members experienced first-hand the reality that the role of business in response to national disasters has not been properly thought through. In preparing this report, the Task Force has assiduously mined the wealth of experience of its members and other executives—completing nearly 100 interviews—in developing its findings.

This report's recommendations fall into three substantive categories: public-private collaboration; surge capacity/supply chain management; and legal & regulatory environment. In addition, the report specifies priorities and sequencing for implementing its recommendations.

During the late summer and fall of 2006, the report, in draft form, was circulated widely and briefed to federal agencies and congressional offices and staff, the White House, senior leaders at the National Governors Association, the National Emergency Management Association and the Association of State Attorneys General, the U.S. Northern Command, professional associations, and corporate leaders around the country. While the conclusions are those of the Task Force, the report benefits immeasurably from comments and suggestions made by our colleagues in government and business.

We present these recommendations in the belief that the failure so far to properly integrate the private sector into government disaster response capabilities, while serious and pervasive, can be remedied. To do so, however, requires a new dedication to effective public-private partnership and, we believe, a

[1] An Incident of National Significance is defined in the Federal National Response Plan (NRP) as an actual or potential high-impact event requiring a coordinated and effective response by an appropriate combination of federal, state, local, tribal, nongovernmental, and/or private sector entities in order to save lives, minimize damage and provide the basis for long-term community recovery and mitigation activities.

new approach: simultaneous, integrated action from *both* the very top of our federal government structure *and* from the state and local levels upward.

This report's recommendations constitute the framework of an action plan to implement this new approach. Its key proposition is that Emergency Operation Centers (EOCs), which already exist at all levels of government to plan for, train and implement emergency responses to disaster, must include a seat for the private sector. The private sector, in turn, must maintain parallel structures, referred to here as "Business Operation Centers (BOCs)" that can plug-in to government operations and "scale up" with them in a *parallel* and *coordinated* manner as government adapts to deal with disasters from small to large. If this structural reform is adopted, it will greatly facilitate all of the other reforms recommended in this report.

As simple and logical as this proposition sounds, formidable political, organizational and legal obstacles now block simple and logical implementation. These obstacles can and must be overcome if we as a nation are to seriously prepare for the next major calamity. Overriding all is the need for Congress to recognize the value of establishing public-private partnerships in concord with state, regional and federal entities and to provide funding through the Department of Homeland Security grant program to sustain them.

The very sinews of American democracy have always resided in the integrity of our close-knit communities, of which business has ever been and remains an integral part. We should not undervalue the power of this bond in an age where our national security is being tested in new and daunting ways. Business must be integrated into our disaster response plans not only because businesses have material assets, money and technical expertise. American businesses are patriotic. They value their community and their nation, and have and will willingly contribute their treasure and talent toward maintaining our cherished way of life.

Key Findings and Recommendations

This BENS Task Force Report focuses on institutionalizing an effective and sustainable role for business in disaster response at all levels of government. To that end, it offers recommendations in three substantive categories:

1. **Public-private collaboration**, to plan, train, exercise, implement and evaluate joint actions required to facilitate effective communication, decision-making and execution;
2. **Surge capacity for private-sector goods and services, and the capabilities resident in private-sector supply chains to manage the delivery** of goods and services (whether pro bono or contracted) to and within disaster areas; and
3. **The legal & regulatory environment**, which can help or dramatically hinder efficient delivery of private-sector support during a disaster.

Public-Private Collaboration

Finding: The American private sector must be systematically integrated into the nation's response to disasters, natural and man-made alike. Government alone cannot manage major crises nor effectively integrate the private sector after a crisis occurs. The Task Force believes that building public-private collaborative partnerships, starting at the state level, is one of the most important steps that can be taken now to prepare the nation for future contingencies. Unfortunately, with few exceptions, durable, collaborative relationships do not today exist.

Consistent with this finding, the Task Force recommends:

A. **Creating new ways to institutionalize public-private collaboration at the state and major metropolitan area levels;**
B. **Facilitating greater public-private collaboration at the regional and federal levels; and**
C. **Building a "Business Emergency Management Assistance Compact (BEMAC)" structure.**

Surge Capacity/Supply Chain Management

Finding: America's existing commercial supply chains can provide a wider range of goods and services on demand than any level of government can possibly match. During national disasters, these supply chains have provided goods and services both with and without payment from an end user. Government at all levels should incorporate such capabilities into disaster response planning. For the most part, government has so far failed to do so.

Consistent with this finding, the Task Force recommends continued efforts re:

A. **Improving government emergency-purchasing protocols;**
B. **Revising deficient donations management systems; and**
C. **Modernizing logistics processes across the board.**

Legal & Regulatory Environment

Finding: Business requires a predictable legal regime to operate efficiently in an emergency situation, whether that business is engaged in charitable or profit-motivated activities. The current legal and regulatory environment is conducive to neither predictability nor efficiency.

Consistent with this finding, the Task Force recommends that Congress:

A. Enact a nationwide body of "disaster law";
B. Modify the Stafford Act[2] to include the private sector; and
C. Hold hearings to determine which Task Force recommendations can be implemented under existing law and which require new legislation.

The Task Force urges government to move quickly to integrate business into its disaster response planning on the federal, state and local levels, and within the operations continuums that link levels of government together. Recognizing that the task is complex, and that political and fiscal limits make it impossible to implement all recommendations at once, the Task Force has identified and prioritized specific desired outcomes and policy drivers in Appendices F-I at the end of this report. This has been done to facilitate the deliberations of political leaders, responsible government officials and private-sector experts.

[2] The Robert T. Stafford Disaster Relief and Emergency Assistance Act (Stafford Act), 42 USC 5121-5206.

Introduction: Background, Methods and Aims

Americans learn only from catastrophe and not from experience.
—Theodore Roosevelt

For a quarter century, Business Executives for National Security (BENS) has served as the principal channel through which senior executives can help build a more secure America. As a national, non-partisan, non-profit organization, BENS has focused on adapting successful models and practices from the private sector to strengthen the nation's security.

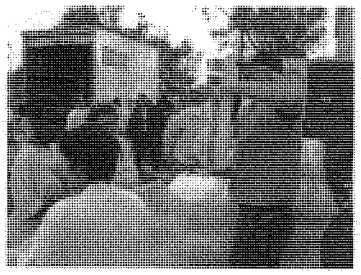
Coming four years after the September 11, 2001, attacks, the hurricanes of 2005 dramatized the frailties of our nation's disaster response system. As the disasters unfolded, BENS was contacted by numerous business executives seeking help in navigating the bureaucratic obstacles impeding them from providing private-sector goods and services to those in need. BENS tried to help, but, lacking established relationships with public-sector responders in the Gulf, successful outcomes were largely elusive.

As the official reports concerning the disasters of the previous summer began to emerge in early 2006, much was said about improving government responses and even about reaching out to business to help. But while these reports were long on rhetoric and generalities, they were disappointingly short on specific plans of action.

So BENS decided to *get down to business*. In June 2006, BENS chartered a Task Force [see Appendix A] comprised of senior U.S. business leaders closely tied to disaster response functions: telecommunications, retail and wholesale supply chains, utilities, manufacturing, real estate, financial services, management consulting and other key industries. The goal, said Task Force Chairman Duane Ackerman, was "to ensure that as recovery occurs at the local level, [the efficient application of private-sector capabilities and resources] are preserved as the disaster escalates and local, state and federal officials are all at the scene together."

The aim of the Task Force was to build up what U.S. Comptroller General David M. Walker, during his March 2006 testimony before the Senate Committee on Homeland Security and Governmental Affairs, called the "total force"—by which he meant the coordinated assets of federal, state and local authorities, the military, non-profit organizations, *and the private sector.*

With the support of the BENS staff and professional assistance provided pro bono by Science Applications International Corporation (SAIC), the Task Force members [see Appendix B] laid out an ambitious agenda for how to approach the task of integrating the private sector into our nation's disaster response system. In order to publish a report that captured the broadest possible range of disaster-related experiences and recommendations, the Task Force asked the BENS staff to design and conduct a comprehensive survey.



Over a 90-day period, interviews were conducted with nearly 100 CEOs, corporate security and emergency management officers, and subject-matter experts with emergency-related knowledge and perspective [see Appendix C]. This survey data formed a baseline record of private-sector response to crises. The survey sampled both small and large businesses in an array of industries and included a number of former senior government officials and disaster response experts.

Survey questions focused on respondents' experiences with Emergency Operations Centers (EOCs), with the pre-positioning of goods and services (either for their own continuity or to assist emergency responders), with

physical access and security issues, and with the escalation of authority from local to state to federal levels. Interviews included discussion about broad or industry-specific legal and regulatory issues that may have impeded the implementation of company continuity plans or the ability of a firm to assist in its community's recovery operations. Interviewers also solicited specific suggestions on how to fix the problems identified.

As survey research proceeded, the Task Force organized itself into three scoping groups to analyze lessons from recent national disasters and to document examples of private-sector disaster response capabilities.

The Task Force survey was revealing. It reaffirmed several truths that Task Force members recognized from their own experiences. First, disasters happen regularly and businesses routinely plan for such contingencies. Second, businesses in disaster-prone areas often have extensive experience collaborating with public-sector first responders. Third, after securing their own operations, businesses invariably move to help ensure the continuity of the community. As such, response from the private sector is typically automatic, not only because businesses are citizens of their own communities, but also because without continuity of community no business can be done.

"We need to know how to connect locally, so that we are not just addressing the needs of our employees and their families, but the needs of the larger community."
– Dr. Mark A. Sanna, Senior Director, Global Security, Kraft Foods, Inc.

The evidence from the 2005 hurricane season testifies to all these truths, particularly the final point. Private-sector assistance during and following the major 2005 hurricanes—Katrina, Rita and Wilma—totaled about $1.2 billion, 25 percent of that in products and services, the remainder in cash contributions from companies, employees and customers. At least 254 companies made cash or in-kind contributions of $1 million or more.[3] In addition, the U.S. Departments of Homeland Security (DHS) and Commerce (DOC), as well as state governments, relied on the business community for reliable information about the situation on the ground. Situation reports provided by business, based on their first-hand knowledge of local infrastructure, geography and geology, helped to shape government's response.

"We don't count on plans, we count on training....[W]e have regular meetings of our emergency people. Live exercises, table-tops, including local first responders and local government officials."
– Donna Shalala, President, University of Miami

In thinking about the Task Force's aims, it soon became clear that the key was determining how to scale effective local responses up to a true national response capability. The nine main themes that emerged from the survey helped Task Force members frame their recommendations.

Preparation: The first theme to emerge from the surveys was that companies' experience in preparing for crises is extensive and applicable to government preparations.

All but the smallest business organizations have a continuity plan in place. For some, that means compiling executive phone lists, buying satellite phones with text-messaging functions, and making contingency arrangements with vendors. Other firms have their own 24-hour emergency operations centers, run live crisis-scenario drills with government agencies

[3] "From Relief to Recovery: The 2005 U.S. Business Response to the Southeast Asia Tsunami and Gulf Coast Hurricanes," U.S. Chamber of Commerce, Business Civic Leadership Center, March 2006.

"You have to learn to expect the unexpected. Not everything will be found in your crisis management manual. For example, nowhere in our crisis management manual did it demonstrate how to get a dead 600-pound sea lion out of your parking lot."
– Lance Ewing, VP Risk Management, Harrah's Entertainment, Inc.

as participants, and develop emergency fall-back plans with their competition so that business can be moved to a remote location in the event of crisis. Nearly all companies stressed the importance of training their employees and crisis management leaders.

Another important aspect of preparation is planning how to distribute goods and services to the people who need them. Major retailers know to stock up on extra supplies during hurricane season and position them just outside the hurricane zone in order to be able to deliver them immediately after a storm passes. Government needs to leverage that private-sector capacity and plan for its use.

Many interviewees stressed that continuity plans need to be flexible and imaginative. Business employees and government officials need to be prepared to operate in unpredictable emergency situations. This involves devising plans that are imaginative enough to deal with a host of different circumstances (such as the failure of levees in New Orleans) and are flexible enough to allow individuals to deal with completely unexpected events.

Relationships: The second theme is that relationships must be established in advance of a crisis.

Companies pursue pre-crisis relationships for their own continuity plans by developing lines of communication among employees and senior executives; with neighbors, suppliers and even competitors; and with government authorities at all levels. Said one interviewee, "you don't want to be handing out business cards...in the middle of an emergency." Many company representatives complained that, based on what they witnessed during the 2005 hurricanes, government appeared to have failed to make connections *even among its own agencies*, not to mention with the private sector.

"[W]e had a very instructive vantage point being the headquarters and watching [the response] grow, and watching the capability and confusion at the same time. I saw how it mushroomed: how complicated it was, how many players there were, how many uninformed players there were, how many inexperienced players there were, how little they communicated, and how often they changed. It's amazing anything got done."
– Patrick J. Quinlan, M.D., Chief Executive Officer, Ochsner Clinic Foundation

The question often posed was that if cutthroat business competitors manage to cooperate in a crisis, why can't government agencies?

Authority: The third theme is that there is a lack of clarity about who is in charge once governmental authority escalates from the local to the state and federal levels.

Federal, state, and local government personnel are all on the scene following any Incident of National Significance, and confusion among them is common and somewhat understandable. Problems with credentialing and permitting, fights among agencies (even those under the same department), and problems related to commandeered goods and equipment are omnipresent. The surveys uncovered a number of stories where a company's trucks were commandeered by one agency while trying to deliver emergency supplies under contract to another. There also were cases where vehicles credentialed by one government authority were denied entry to the disaster area by another government authority down the road. There were many cases where two or more agencies, regardless of government level, would butt heads over turf issues in the midst of a crisis.

One organization told an interviewer that while the Federal Emergency Management Agency (FEMA) was, figuratively, at one door to help, the Customs and Immigration Service (CIS) was at the other, trying to remove employees whose visas were invalidated because the organization was closed for business (even though closure was due to the very same hurricane that its fellow DHS agency was addressing via recovery efforts).

"We're competitors, not enemies. We collaborate during emergencies.... We had one competitor who gave us office space, and we'd do the same for them. Relationships were all in place beforehand."
– Gregg Jones, Chief Administrative Officer, Greenberg Traurig, LLP

Communications: The fourth theme is that operational and accurate communications are vital.

Crisis wreaks havoc with technology. From 9/11 to Wilma, we were told that phones and computers do not work (either because of a lack of electricity or because satellite, cellular and land lines have crashed). People cannot physically move to back-up communications locations because of evacuations or public-safety concerns. But the problem transcends technology. During Katrina, even when a company could feed into a government source or EOC, it was reported that the information available was often confusing and inconsistent, particularly when multiple government authorities were on hand.

Interviewees differed on what would constitute an ideal arrangement for coordinating communications. Some preferred that one voice speak on behalf of all government to the private sector; others preferred to gather information from multiple sources and sort it out on their own. All concurred on three points, however: that more organized communication between government and business needs to occur; that government personnel must be clear about what they need; and that officials placed in a communications role must have the authority to make quick decisions.

"On the communication side: If the land lines aren't working—which they are not if the power is down—you will only have cell phones. Whatever system you have, they have two problems: one, the power to the towers went down, and two, their backup batteries only had a short useful life.... So in any business that is spread out...you're basically out of business. This season all of the senior executives have three separate cell phones on different systems, hoping that at least one of the systems will be up and operating in the areas where we need it."
– Gerald D. Kelfer, President & CEO, Avatar Holdings Inc.

Logistics: The fifth theme is that a need exists for improved methods to deliver goods and services to the government or directly to needy communities during crises.

Interviewees discussed at length government's inability to accept and distribute goods and services in an efficient manner following Katrina. Everything from food and clothing to medical care came in, but without control over the distribution system, ice melted, donated clothing piled up and rotted, and medical personnel were turned away. One company had 600,000 tarps available to cover damaged roofs, but the federal government was unable to draw on the supply chain to secure and distribute them. Another company offered to donate three mobile communications units, only to be told that their offer was refused and then countered with a request to buy ten of the same. We were told by one interviewee that a senior manager of a large transportation association spent a full day trying—and failing—to locate a single authoritative point of contact within FEMA to coordinate bus deployments. Numerous examples were cited of the government's inability to accept private-sector donations, often because of a lack of pre-defined procedures or mechanisms for doing so.

Interestingly, many companies we interviewed had not heard of DHS' National Emergency Response Registry (NERR). The NERR, created during

"You go to war with the army you have. The problem in Katrina was that the FEMA army was ill-equipped for the job, and the lesson we took away from it was that we have to marry the private sector and the public sector before the disaster occurs, otherwise those resources will not flow and will not be made available. Once the disaster occurs, it's too late to begin to develop personal relationships, and to put in place the systems that are necessary that will facilitate the people at the federal side and state and local sides, working with the private sector."
– Peter F. Carpenter, President, INSTEDD

"Have you heard the FEMA Bob and FEMA Joe stories?...The way people down here learned to deal with FEMA was to just talk to them more than once. FEMA Joe will tell you one day that you can't do this, but if you go back the next day and talk to FEMA Bob, he'll tell you that you can."
– John McFarland, Marketing Director, The *Biloxi Sun Herald*

the Hurricane Katrina response, was an Internet-based system to source goods and services to the government during emergencies. Most interviewees expressed support for the concept but wanted to know why the NERR was kept a virtual secret from businesses, given that DHS sought to implement such a system. That frustration also was reflected by some in government.

Other companies discussed concerns about government contracting, with many stories about procurement process problems. Surprisingly, complaints never focused on payment issues (although some companies reported very long delays in FEMA reimbursements). Rather, many companies were perplexed by rules requiring federal government agencies—but not states and localities—to refuse pro bono donations and demand for-fee contracts instead. Still other complaints noted that work offered at one fee was sometimes rejected in favor of the same work paid at a *higher* fee—which some companies regarded as unconscionable. For example, one large restaurant chain offered to distribute boxed lunches at a price of $4.50 per lunch but ultimately rescinded the offer when FEMA refused to pay less than $6 per lunch. Many of these problems stemmed from government procedures that tied the hands of FEMA officials. However, it also was reported that many government contracting officers seemed to be unaware of the variety of contracting vehicles available to them during crises, and either did not know how to streamline the contracting process or were not empowered to do so.

Business response: The sixth theme is that like government authorities, companies also play the role of first responders and thus need to be given priority status.

The private sector plays a critical role in post-disaster community reconstruction. Disasters often destroy many key components of a community's critical infrastructure, and business continuity for companies in those industries (such as energy and telecommunications) is an essential component of the community's immediate recovery. Therefore, these corporate first responders (identified as such by the authorities and prior to a crisis) need to be given priority status with regard to credentialing and access to facilities, affected areas, and information. Many interviewees also proposed that banks and waste removal services should be added to this list of corporate first responders, since two repeatedly-mentioned areas of post-disaster civil unrest concerned cash and garbage pick-up.

Because the private sector plays an essential role in rebuilding the community, it is important that government agencies generally refrain from commandeering essential goods from corporate first responders. Many interviewees specifically complained that government officials often commandeered their backup fuel tanks. Fuel and power frequently were cited as the most important resources needed early in a crisis. Without those inputs, business cannot proceed—and many continuity plans fall apart. Some interviewees also suggested that laws be enacted to require gas stations to install emergency generators, ensuring that they can pump their own fuel in emergency situations.

FEMA: The seventh theme is that FEMA must make dramatic improvements in the planning and coordination of its recovery efforts.

Nearly all respondents asserted that FEMA failed in its efforts following Katrina. There were a few good stories shared, but all agreed on two points. First, FEMA representatives were replaced far too often, which resulted in FEMA policies being inconsistently applied and the establishment of working relationships with FEMA on the local level becoming nearly impossible. Second, the mechanisms for establishing two-way communications with FEMA officials on the ground were unreliable from the start and quickly overwhelmed.

"If you start reading the 300-page National Pandemic Flu Plan, they categorize and prioritize different categories in terms of what they think is critical infrastructure—garbage men are level 6, which is almost at the bottom. You'd think we'd be up there with critical utilities because that's basically what we are, but we're not. We're down there below everybody and their brother."
– Michael R. Lambert, Corporate Director of Safety, Republic Services, Inc.

The Good Samaritan: The eighth theme is that the vast majority of companies—like the vast majority of citizens—will strive to "do the right thing" during crises.

When asked about their Good Samaritan actions, most companies simply said that they aimed to do the right thing and worried about the monetary and regulatory implications later. When asked what aspect of previous disaster recovery efforts they are proud of most, companies said that it was being able to help their communities and their own employees.

One can discern from this feedback that organizational cultures that are not risk-averse in their daily behaviors will not be inclined to be risk-adverse in a crisis. The challenge is how to transfer this cultural insight from the private sector to government bureaucracies.

Legal and Regulatory Barriers: The ninth theme is that regardless of industry, size, or location, companies found significant regulatory barriers that hindered their ability to execute their own continuity plans, to assist within their communities, assist other communities, and work in concert with government recovery efforts. Some of those impediments, such as permitting and credentialing, have been mentioned above. Others involved financial filings, gasoline mixes, health inspections, and much more. In fact, the interviews uncovered far more than we could catalogue in this report. In many cases, government authorities waived regulations that would prove to be unnecessary or overly burdensome in the midst of crisis. In others, the government did approve the waiver—but only after weeks of meetings in Washington. Of course, there also were reports of laws and regulations not being waived at all, leaving companies in fear of legal reprisal should they act to "do the right thing" versus consulting their legal counsel first.

"If you've got twenty employees in your firm, and you are trying to give them some cash so that they can take care of their families—they might not have a home, they might not have a car, they might not have a place to stay—you try and give them $500 each—that's $10,000, and you've got to fill out a...currency transaction report—for an established customer! That's my pet peeve, and you can't get...Washington to even think about: if it is a national disaster, waive it for a week, waive it for...two week[s] for an established customer."
– Chevis Swetman, Chairman, President & CEO, Peoples Financial Corporation

The three Task Force scoping groups set out to develop recommendations that flowed from their own experience. Informed by these nine insights, they focused on developing key questions for deliberation. They are:

Public-Private Collaboration

- How can business become better integrated structurally into the disaster response effort?
- What mechanisms can improve how business and government communicate and coordinate decision-making before, during and after a crisis, at all levels of government?

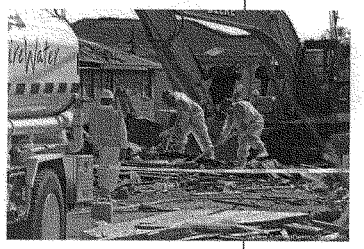
Surge Capacity/Supply Chain Management

- How can government improve contingency contracting and pre-qualification of vendors for goods and services that will likely be needed?
- How can government and business facilitate and accelerate the delivery of resources (assets and volunteers) that business offers on a pro bono basis?
- How can business emergency-response resources be deployed and managed by federal, state and local government agencies to maximize speed and utility and minimize redundancy?

Legal & Regulatory Environment

- How can government improve Good Samaritan laws to better protect businesses and their employees who volunteer to help?
- How can legislation, regulation and policy be better aligned at the federal, state and local levels to encourage private-sector preparedness and better mobilize the private sector in a catastrophic event?
- Is revision of the Stafford Act desirable?

After assimilating the results of the Task Force survey, each scoping group developed recommendations for the *near term* that optimize business participation in disaster response. They also developed recommendations for the systematic *longer-term* integration of the private sector into the National Response Plan and its execution in a disaster.



These recommendations are presented in the following three chapters. A fourth chapter—an "Expert's Guide to Priorities and Sequencing"—describes a path for systematic private-sector integration consistent with the federal government's revised NRP; it is the Task Force's summary statement of the actions required to implement the recommendations in this report.

Chapter 1. Public-Private Collaboration

Finding: The American private sector must be systematically integrated into the nation's response to disasters, natural and man-made alike. Government alone cannot manage major crises nor effectively integrate the private sector after a crisis occurs. The Task Force believes that building public-private collaborative partnerships, starting at the state level, is one of the most important steps that can be taken now to prepare the nation for future contingencies. Unfortunately, with few exceptions, durable, collaborative relationships do not today exist.

Consistent with this finding, the Task Force recommends:

A. **Creating new ways to institutionalize public-private collaboration at the state and major metropolitan area levels;**
B. **Facilitating greater public-private collaboration at the regional and federal levels; and**
C. **Building a "Business Emergency Management Assistance Compact (BEMAC)" structure.**

Local, state or regional public-private partnerships are vital to filling gaps in homeland security and disaster response that neither government nor business can manage alone. These partnerships mobilize private-sector cooperation—including the supply of material assets, volunteers, information and expertise—that strengthens our nation's capability to prevent, prepare for, and respond to catastrophic events.

For responding to disasters, the private sector encompasses the for-profit business community in all its aspects. Those aspects include critical infrastructure,[4] the disaster response supply chain,[5] and other business sectors (e.g., architecture and engineering firms, the hospitality industry, mortuary services) that may be called on for support in a crisis or that are necessary for the continuity of community in the aftermath of a disaster.[6]

Ensuring continuity of community is essential for recovery from disaster in all forms. Good will aside (and there were innumerable examples of companies acting out of nothing more than corporate citizenship), although most businesses plan for rebuilding and restoration of operations and for the safety and security of employees, they also recognize the interdependencies that exist in communities. A functioning community is

"Public-private partnerships are truly the best way for America to imagine solving its problems down the road, [including both] the simplest notion of a standard setting responsibility, being that of the federal government, and the real generation of solutions to problems being forthcoming from the private sector—the link between the two is the ultimate public-private partnership that will be the answer to so many of our challenges."
– Admiral James M. Loy, USCG (Ret.), Senior Counselor, The Cohen Group

[4] Critical infrastructure includes: 1) Agriculture, food (meat, poultry, egg products); 2) Public health and healthcare; 3) Food (other than meat, poultry, egg products); 4) Drinking water and wastewater treatment systems; 5) Energy, including the production, refining, storage, and distribu-tion of oil and gas, and electric power (except for commercial nuclear power facilities); 6) Banking and finance; 7) National monuments and icons; 8) Defense industrial base; 9) Information tech-nology; 10) Telecommunications; 11) Chemical; 12) Transportation systems; 13) Emergency services; 14) Postal and shipping; 15) Dams; 16) Government facilities; 17) Commercial facilities; 18) Nuclear reactors, materials, and waste.

[5] The Disaster Response Supply Chain consists of commercial suppliers, distributors, and vendors at the wholesale and retail level.

[6] Non-governmental and charitable organizations are also critically important to disaster-response efforts, but their role is beyond the scope of this Task Force.

best defined by its natural commercial and social relationships, and can be a locality, a state, an urban area within a state, or multiple states. If business is to reconnect with its customer base, care for employees, restore operations, and recover quickly from a catastrophic event, it has a clear incentive to participate in the community response to disaster.

Whether activating established distribution networks or deploying aid quickly in the aftermath of a disaster, the private sector can play a critical role in securing communities nationwide. The private sector also needs—and can provide in return—disaster information, coordination of access, protection and prioritization of resources (e.g, fuel). A further benefit is that private sector emergency resources can improve overall situational awareness—if they are tied into the local, state and federal systems. Established partnerships work because they enable business and government leaders to work together not just once but on an ongoing basis across many initiatives and all industry sectors.

Government and business know intuitively that they need to work together during crisis, but how to do so does not come without effort on both sides. Business-government collaborations require a level of trust and agility that is easiest to build at the local, state and regional levels and possible at all levels. It is important that local communities be as self-supporting as possible in their crisis-response capacities, putting a high premium on the efficiencies to be gained through cooperation; federal response capabilities may be quickly overwhelmed if Washington were faced with several simultaneous incidents.

"[Y]ou have to recognize the strengths of the various areas...And those strengths are not the same. [T]here is no reason to expect government...to be as good at military deployment as the military is. The point is that businesses are better able to execute on certain things, the military is better able to execute on some things, and government is better able to execute on some things. And the question is how you link them up and take advantage of those various strengths. The failure was access to tremendous resources that were just under-utilized or never accessed because there was no communication and there was no imperative to pull them in."
–Thomas A. Oreck, President, Oreck Corporation

At the same time, business must adopt new methods of cooperation to support federal emergency response efforts. New structures are needed for this purpose, and among these, regional public-private partnerships can be critical in helping to sort through the multiple and overlapping requests from federal, state and local government agencies that arise in a crisis. Regional arrangements can allow business and government leaders to better coordinate requests from multiple government agencies and to develop coherent disaster response plans according to the needs and priorities of their respective regions.

A. Institutionalizing Public-Private Collaboration at State and Major Metropolitan Area levels

The purpose of state Emergency Operations Centers (EOCs) is to facilitate coordination among essential government personnel during a crisis. Through its emergency and disaster grants program, the federal government has encouraged states to develop EOCs.[7] Many states and cities have indeed developed such capabilities, as have major utility companies. The Task Force recommends that those states, cities and other critical infrastructure entities that have not should do so promptly.

[7] Public Law 107-206, "2002 Supplemental Appropriations Act for Further Recovery From and Response To Terrorist Attacks on the United States." Phase 1 grants of $50,000 to each state are used for an initial assessment of the hazards, vulnerabilities and resultant risk to existing EOCs. Phase 2 grants address the most immediate deficiencies and require a 50 percent non-federal cost share.

Like government, most major (and many smaller) retailers and vendors in the disaster supply chain have their own emergency operations centers. These centers provide a location where employees in charge of emergency management can communicate with the workforce and make important business continuity decisions. Among the companies that do not have EOCs, most still have emergency communications, protection, and restoration plans. The extent of business continuity planning varies among industry sectors and among individual businesses.

Because government has EOCs to coordinate emergency response, and because the private sector has its own EOCs and emergency restoration plans, it seems logical that government should use its EOCs to tap into the vast organization of emergency resources and communication networks the private sector can offer. Thus, the Task Force recommends that every state and major metropolitan EOC offer a seat at the table—or broaden representation if it already exists— for at least one business representative to serve as liaison to the business community at large. This representation should complement, not replace, presence in the EOC granted currently to public utilities. Further, the Task Force recommends that a Business Operations Center (BOC) be established to operate in conjunction with each EOC, to provide a forum for collaboration, coordination, and decision making between the public and private sectors.

Participation in the BOC should represent critical infrastructure and other industries/companies vital to community viability and continuity in crisis situations. Recognizing that it is not possible for all businesses to participate at the "table" at once, the Task Force recommends that BOC membership be generally rotating and structured in three tiers:

1) Critical infrastructure owners and operators as permanent members;
2) Other sectors or companies deemed critical to restoring the continuity of community, represented as necessary (these seats could be rotating or permanent, based on the number of such businesses or the nature of the functions they provide to the community); and,
3) Entities representing business at large within the community (Chambers of Commerce, professional or trade organizations, or civic clubs, e.g., Rotary), as rotating participants that can reach back to their business membership for help or information sharing.

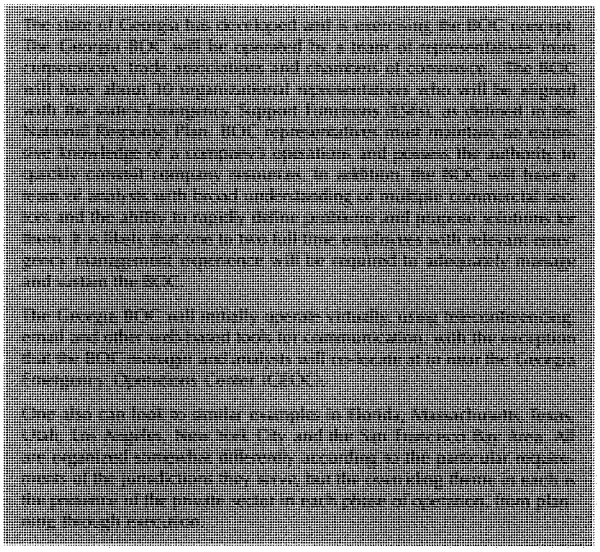
The BOC concept creates an operational capability that integrates private-sector resources into emergency response plans. It is precisely this operational capability that is missing from the National Response Plan as currently constructed—despite the frequent exhortations in federal reports that the private sector be included. A BOC, connected structurally to its corresponding EOC, will greatly enhance disaster-response capability by providing a vehicle to include the private sector in planning, preparation, training, exercises and execution.[8]

"A new topic [in disaster response] is 'cross-industry response.' The telephone companies can only do so much on their own, because eventually they rely on the power companies, who in turn rely on some other industry such as the transportation industry. [W]e need to consider what happens to the other related industries such as the financial industry, [which is] dependent on the transmission of data among their various sites. Working together on a cross-industry basis is the only truly complete solution."

– Larry Babbio, Vice Chairman and President, Verizon Communications, Inc.

[8] Although outside the Task Force's purview, our assessment suggests that EOCs also should have substantial non-governmental organization (NGO) representation. Many EOCs have a seat for the American Red Cross and Voluntary Organizations Assisting in Disaster (VOADs), which include NGOs and faith-based organizations; however, participation is not consistent across the country.

The Task Force believes that to ensure that the BOC concept spreads nationwide, the Congress should direct DHS to create guidelines and funding for states and urban areas to build BOCs. Public-private communications systems and data interchanges may require direct appropriation. However, sustaining funding through the DHS Grants & Training program should be tied to the states and urban areas developing, training and exercising the EOC-BOC collaboration.

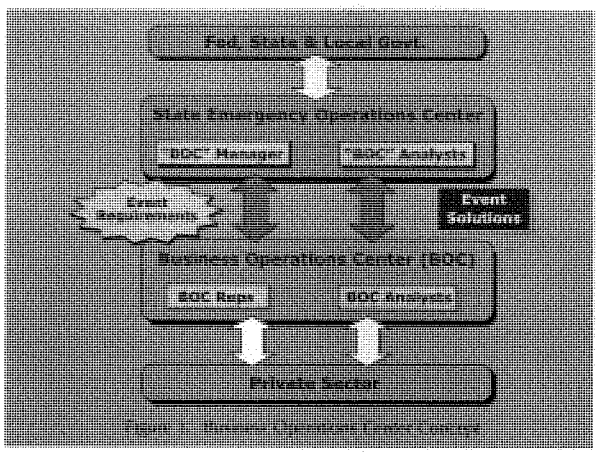


Recommendation:

A. Integrate business into existing and prospective Emergency Operations Centers (EOCs) of states and large urban areas through the establishment of Business Operations Centers (BOCs).

1. Formalize a business presence in state and urban emergency operations centers, to include emergency planning, training and testing through periodic drills.

2. Include Critical Infrastructure sectors, if not already represented, and those industry sectors not classified as critical but typically a part of the disaster response supply chain (e.g., retail and wholesale), and other critical businesses, such as the service and hospitality industries. Businesses need cross-sector links to one another and the credentials and clearances to operate with state and local EOCs before, during and after a catastrophic event.



"Prior to the federal government getting involved, most communities have a local plan that has local players that have relationships and know what to do, especially around critical infrastructure. Once that process is overwhelmed, that's where the issue begins to get complicated....That's when...the problem escalates in terms of degree of complexity, and all the relationships between the federal government and the state, the federal government and the private sector, [and] the federal government and the city become the issue at hand."
– Duane Ackerman, President & CEO, BellSouth Corporation

3. Congress should tie this requirement to receipt of federal homeland security grants/funds.
4. Require testing, training and exercising of a formal business presence in state and local emergency operations centers to ensure proper functioning in a crisis.
5. Ensure that the BOC remains a permanent entity by codifying it in the National Response Plan, sustained by the DHS-sponsored grants program.

B. Facilitating Greater Public-Private Collaboration at Regional and Federal Levels—Scaling-up to an Incident of National Significance

Unless their operations are compromised or incapacitated, state and local governments are likely to have the first look at what goods and services are needed during a crisis. They are responsible for transmitting this information to public and private relief organizations.

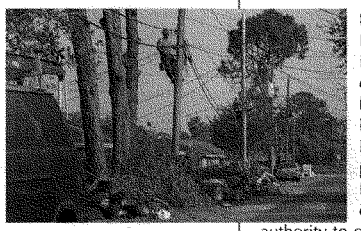
If, however, a disaster rises to the level of an Incident of National Significance,[9] the resources of the federal government are brought to bear. The introduction of federal resources and authority presents the challenge of "scaling-up" to accommodate a new set of players without loss of efficiency.

Within the National Response Plan, the mechanism for this "scaling-up" process is the Joint Field Office (JFO). Before we face another disaster, it

[9] The National Response Plan recognizes the potential magnitude of threats from weapons of mass destruction and severe natural disasters by adoption of a new term, the Incident of National Significance. An Incident of National Significance is described as an incident with high impact requiring an extensive and well-coordinated response by federal, state, local, tribal, and nongovernmental authorities to save lives, minimize damage, and provide the basis for long-term community and economic recovery.

must be resolved how business will "plug in" to the plan as DHS organizations and the U.S. Northern Command (NORTHCOM) come into the mix through the JFO. To smoothly transition from local and state operations to federal presence, business-government relationships and roles within the JFO must be more than predetermined; they must be practiced.

This recommendation sounds straightforward, but in truth, the task is both challenging and complex. Government and the private sector must work together to identify, in advance, governmental needs and the resources available to match them. Roles on both sides must be clear, and each entity must play to its strengths with as little mutual interference as possible. When possible, government must provide information on required goods and services, access to disaster sites, and security for relief workers in the area of operations. The private sector must in turn be prepared to execute its supply chain operations according to established procedures, with the least possible regulatory interference and with reasonable protection from legal liabilities.



DHS recently established a liaison to the critical infrastructure Emergency Support Functions (ESFs).[10] The JFO has a critical infrastructure liaison position intended to interface with all critical infrastructure companies—but one individual cannot handle all of the activity generated in a crisis. That is why DHS should establish a private-sector position linked to a BOC-like concept in the JFO and establish an ongoing public-private relationship in each of the ten FEMA regional offices. In both cases, two conditions must be met for the liaison to be effective: the business designee(s) must have sufficient authority to commit the businesses they represent to take action; and the government, especially in the JFO, must recognize that BOC input deserves serious and high-level attention.

The Task Force believes that to build enduring public-private collaborations at the regional and federal levels Congress needs to direct DHS to create guidelines and provide funding for such entities.

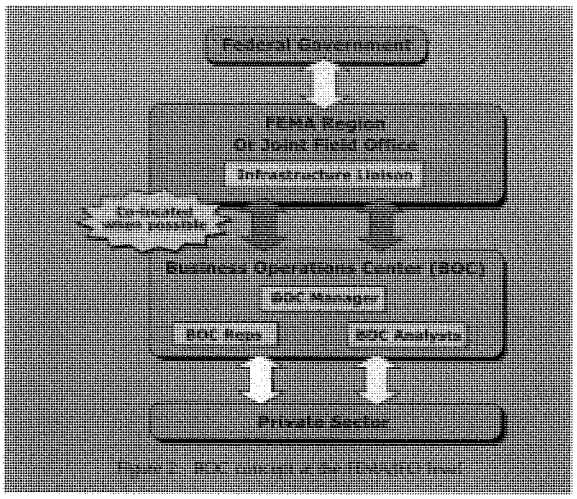
Recommendation:

B. Facilitate greater public-private collaboration that will continue as disaster response and recovery activities escalate to include federal components under a Joint Field Office structure.

1. Establish long-term solutions that fully integrate the private sector with regional entities and federal agencies, including creation of a Business Operations Center (BOC) model at the JFO and/or FEMA regional level. Recognize that a single event spanning multiple regions or multiple events in different regions may require the operation of more than one JFO/FEMA-BOC structures.

2. Establish a common set of private-sector expectations and "rules of engagement" consistent with local, state and federal roles,

[10] Emergency Support Function 15 – External Affairs has been modified (July 2006) to include the private sector.



responsibilities and methods of operation. Broadcast these standards widely and conduct necessary training and practical exercises, so that they are thoroughly understood in advance of an actual disaster.

3. Weave the above recommendations into a strong fabric of business-government collaboration on a nationwide basis:

   a. Create regional partnerships with common elements and local flexibility to provide the resources, structure and local commitment needed to implement and exercise Task Force recommendations on a sustainable basis.

   b. Ensure BOC personnel understand and complete training under the National Incident Management System (NIMS).

   c. Provide outcomes-based federal funding to enable regional partnerships to implement and exercise the above recommendations and share best practices across the country.

C. A Business Emergency Management Assistance Compact

A successful example of a national mechanism for matching needs with available resources is the state mutual-aid program known as the Emergency Management Assistance Compact, or EMAC. EMAC currently enables affected states to request government resources from non-affected states, and it obliges non-affected states to comply if they are able.

The EMAC program could and should be expanded to include private-sector resources. An expanded EMAC program could knit together a fabric of state-based Business Operations Centers to create a scalable, flexible and robust

"[EMAC has] existed since Hurricane Andrew. We test it every year, we exercise, we have written policy manuals, guided direction; it really can serve as a model for that kind of provision. It's simple but robust, and that's ultimately what we're talking about when it comes to private-public partnership."
– Mike Sherberger, former Director, Georgia Office of Homeland Security/Georgia Emergency Management Agency

"network of networks." Trained private-sector representatives would work alongside emergency management leaders to coordinate government and private-sector resources using interoperable processes and technical tools (e.g., same communication systems, same data exchange systems, etc.). This program would provide the mechanism for identifying in advance and rapidly deploying billions of dollars of business resources on a nationwide basis.

[illegible]

Recommendation:

C. Build a Business Emergency Management Assistance Compact (BEMAC) Structure.

1. Expand existing FEMA and state models to better forecast the resources and capabilities that are critical in the early stages of a disaster.
2. Create state and regional resource registries of private-sector resources, including resources government expects to purchase and those that business expects to provide on a pro bono basis during catastrophic events.
3. Create a mechanism similar to EMAC to connect business resources in unaffected states to states in the disaster zone.
4. Create business support teams similar to EMAC "A-teams," which send emergency management officials from outside the disaster zone to the affected state(s).
5. A BEMAC system should complement, not replace, existing mutual aid processes like those in place in the public utilities sectors.

Chapter 2. Surge Capacity/Supply Chain Management

Finding: America's existing commercial supply chains provide a wider range of goods and services on demand than any level of government can possibly match. During national disaster, these supply chains have provided goods and services, both with and without payment from an end user. Government at all levels should incorporate such capabilities into disaster response planning. For the most part, government has so far failed to do so.

Consistent with this finding, the Task Force recommends continued efforts re:

A. Improving government emergency-purchasing protocols;
B. Revising deficient donations management systems; and
C. Modernizing logistics processes across the board.

"If something is disrupted, [there must be a] plan for reconstitution that makes sense, rather than 'first come, first served' or 'we're bigger than you are.' "
– Bruce Townsend, Corporate VP, Security, FedEx Corporation

In the wake of recent national disasters, government agencies at all levels have tried to prepare themselves for future contingencies by forecasting needs and arranging to secure resources. Unfortunately, with the exception of critical infrastructure, the role of the private sector remains unscripted and untested—despite the fact that the private sector is the ultimate source of the materiel and commercial services that will be needed.

The nation must do much more to develop the "emergency marketplace" in advance of the next crisis. To do so, four overarching principles should apply:

- The private sector routinely operates efficient supply chains; government should not be expending time, effort, and money to build its own.
- The goal is to get product to the disaster zone quickly and at fair market price.
- In the disaster zone, the private sector must be granted access and know that adequate security will be provided.
- More planning needs to be put into "last mile logistics."

A. Improving Emergency-Purchasing Protocols

Business prepares for disaster by developing relationships with public officials in the community and knowing what emergency services are locally available. It plans for protection of its business infrastructure and merchandise, as well as for the safety of its employees. Many businesses have methods of maintaining or re-establishing contact with employees so that business continuity can be readily restored. When warning is available, major supply chains, using point-of-sale data from previous disasters, begin moving necessary products towards a disaster zone in advance of need. They also develop contingency contracts or agreements to obtain goods and services that are likely to be needed in case of emergency.

Like business, government can predict some (but not all) of its needs prior to a crisis. And like business, government can and should plan ahead to have

those needs filled in the wake of a disaster. To do so, it must communicate its projected resource requirements to its suppliers. Armed with such information, commercial relationships between the private sector and governments at all levels can be pre-negotiated for those goods and services; examples include electrical power, communications capabilities, engineering/construction, equipment maintenance, field services (e.g., lodging, food services and sanitation), security, medical services, mortuary services, supply operations, and transportation.

Many localities and states have already entered into contracts with the private sector to provide these crisis and post-crisis goods and services. Likewise, the Federal Emergency Management Agency (FEMA) has contracts in place to provide the most common commodities (like water and ice) that are needed following a disaster.

"I find it sadly humorous that the media was so surprised that some great American companies... were really good at the logistics of this. What do you think these people do for a living? They're not $200 billion companies because they're stupid!"
– A restaurateur affected by Hurricane Katrina

The disaster recovery agencies should establish blanket purchase agreements with the suppliers of emergency materials, thus making the contracting process quicker and more efficient. Regardless of the type of pre-qualified government contracting vehicle, however, the contracting officers must be trained, ready, and authorized to make quick decisions within the bounds of those arrangements.

In November 2006, the General Services Administration (GSA) consolidated its emergency response resources into a new Office of Emergency Response and Recovery, providing a central location from which it can support first responders, emergency workers and recovery teams. For both routine purchasing and emergency contracting, some companies have elected to become certified suppliers to the federal government through the GSA Federal Supply Schedule. This mechanism avails the federal purchaser access to thousands of pre-qualified vendors who hold "schedule" contracts with GSA that establish purchasing mechan-isms and commercial pricing similar to catalog buying. By virtue of pre-certification, GSA Schedule vendors will likely be preferred by government purchasers and receive "first bite." To further consolidate buying opportunities, GSA introduced a Disaster Relief and Emergency Preparedness Category to its popular online storefront, *GSA Advantage!*® Of note, the FY 2007 National Defense Authorization Act (PL 109-364, Sect. 833) allows states and localities to purchase from the GSA Schedule to facilitate recovery from natural disasters (as declared by the President), terrorism and certain types of attacks.

Beyond that GSA Schedule pool, there is an even larger vendor market that must be accessible in a crisis. In the first week after a crisis, materials availability is paramount. Many capable vendors in a disaster area may not have undergone a GSA certification, and those that have may no longer have the capability to deliver on their pre-crisis agreements and contracts. This Task Force recommends that in addition to the multiple contracting schedules, government must improve its access to the national commercial marketplace for additional support in a crisis. For example, FEMA should pre-qualify vendors after studying the use of qualified bidders lists (QBL) in accordance with the authority established in the Federal Acquisition Regulation (FAR). The supply chain would benefit from a rigorous and adaptable qualifying and pricing process identified and implemented in advance of the need.

Also, the public sector should recognize and capitalize on the ubiquity of large-scale retailers likely to be in or near the disaster zone. Such retailers should be preferred when they are unmatched in terms of materials availability and quick delivery, advantages that are not readily duplicated in the public sector.

Contracting officers also must become better at using the emergency contracting authorities available to them in the FAR. In May 2003, the Office of Federal Procurement Policy (OFPP) published guidance on the use of emergency procurement flexibilities to help ensure that agencies could effectively meet the demands associated with fighting terrorism. The OFPP is currently updating its guidance to also address flexibilities relevant to other emergency situations. With the guidance in place, it is important for contracting officers to be trained and tested, just the same as first responders, in any emergency preparedness exercises conducted at local, state and federal levels.

While pre-contracting for emergencies has been improved—especially at the federal level, in the wake of Katrina—the Task Force believes that more can be done to leverage the vast resources of the private sector in a crisis. The mechanism most in need of development between government and the private sector is a means to deliver commercial goods in a crisis in a timely and cost-effective manner. As stated at the outset of this chapter, existing commercial supply chains provide a wider array of goods and services than the government can match. It is not evident that government has fully leveraged these private-sector resources in its planning. This process must allow for the effective use of vendors present in affected areas that have the existing/surviving infrastructure to deliver within the "last mile."

"We had to fight for fuel with the government and [other companies] – even though we were all on the same team. We're all calling the same five guys to get the same things. It would be far better if there were a pre-positioned supply chain."
— Robert S. Boh, President and CEO, Boh Bros. Construction Co., LLC

Recommendation:

A. Improve forecasting for emergency goods and services, putting more pre-contracts in place and pre-qualifying vendors.

1. Have FEMA, with the help of state emergency organizations, other DHS offices and the private sector, improve forecasting models for the most critical items needed during the initial response to the most likely emergencies/crises:

   a. The models should be data-driven from recent experience. Most major retailers have vast point-of-sale databases that capture the consumable items most in demand before, during and after a crisis. These could be provided to modelers through industry trade organizations.

   b. Engage major retailers, or their association representatives, in the construction of scenarios covering a variety of events and magnitudes.

2. With the above list, FEMA should work with vendors to establish pricing mechanisms that would set prices during the crisis period at the market price in effect immediately preceding the emergency. Electronic markets exist so that price lists for some commodities could be updated routinely to address normal pre-emergency price fluctuations. States and local municipalities would agree to use these price lists in time of emergency (an example is the routinely updated system of "Average Wholesale Price" used in the pharmaceutical industry).

   a. Establishing a schedule, whether derived from "Average Wholesale Price" or another method, works well in stable times and for certain product categories. AWP is a "warehouse" price and is not applicable to retail pricing, however. As described in the FAR, schedule pricing cannot change just because of a crisis; rather, in order to increase pricing, the contract would need to contemplate the increase.

   b. For many "consumable" categories, like groceries, implementing a schedule or price list is not feasible. Commodity prices can fluctuate rapidly based on changing market conditions after a crisis. Likewise, transportation costs also may change significantly due to the rising cost of fuel, contributing to an overall rise in the cost of commodities. As a result, schedule pricing could cause product shortages in a true catastrophe or in a crisis of long duration. Therefore, FEMA should work with vendors to establish a business-oriented pricing mechanism allowing the government to make rapid product selection decisions. The system should involve pre-qualification of the prospective vendors and then take into account the factors of 1) vendor's stated price, 2) vendor's availability (when can it be delivered in the desired amount at the desired location?), and 3) government's assessment as to the reliability of the vendor. With the proper pre-qualification of vendors (e.g., use of a QBL), requests by government can be

transmitted and vendor responses received and processed quickly.

3. Many major retailers and some states already have pricing policies that take effect automatically in a declared disaster zone. States, working through national organizations like the NGA, should take the lead in developing pricing mechanisms to be implemented in disaster situations and areas. Decisions to implement pricing policies can be tied to a state or national declaration of emergency. Rules should stipulate the duration of the pricing policy and procedures to modify the duration if conditions change or do not materialize. The decision to return to normal operation can be made by the states, in conjunction with the private sector. (As a rule, price blocks should be geographically based on where the crisis exists. Different areas reconstitute more quickly than others and can be released from price blocks more quickly). Such "anti-gouging" regulations should aspire to national standards to both streamline and simplify their implementation, but states—not the federal government—should take the lead in their development.

4. GSA Schedule vendors may opt to take increased inventory positions on certain Stock Keeping Units (SKUs)[11] prior to forecast events (e.g., hurricanes) or long shelf-life items for other kinds of emergencies. FEMA and/or state EOCs would work with the private sector to assess and monitor pre-emergency inventory buildup:

   a. The private sector will pre-stage appropriate inventory levels when possible before the event and will be moving inventories rapidly after the event. Effective communication between the private sector and government is essential to ensuring that the right amount of product ends up in the right place.

   b. It is imperative that government enable the private sector to leverage the flexibility of its supply chain to meet crisis needs. Creating large "stockpiles" of government purchased and warehoused merchandise is neither effective nor advisable.

5. The government, through the Federal Trade Commission (FTC) or other relevant authorities, should consult with private-sector groups as needed to review the list of required items developed in recommendation A.1 above to determine and grant conditional waivers to any trade and regulatory restrictions. For example, provisions of the Trade Agreement Act and Buy America Act may restrict rapid responses to crisis. These waivers must be pre-defined so that they can take effect automatically upon declaration of an emergency.

6. To increase the pool of vendors, government should establish mechanisms for pre-qualifying non-GSA vendors prior to a crisis and for qualifying non-GSA vendors during a crisis:

[11] SKU: An identifier used by merchants to permit the systematic tracking of products and services offered to customers

a. For purposes of pre-qualifying vendors, the Federal Acquisition Regulation provides authority for agencies such as FEMA to use QBLs. FEMA should explore the use of QBLs or similar mechanisms for pre-qualifying vendors.

b. For the purposes of qualifying vendors during a crisis, a simplified certification process based on business information maintained by commercial analysis firms (such as Dun & Bradstreet) and a civil/criminal background check could be employed. Qualification requirements should be tailored to maximize the purchaser's access during a crisis to vendors with product availability and quick delivery windows. The emphasis must nevertheless be on pre-qualification because it is inherently difficult to qualify vendors during a crisis.

c. In extremis, FEMA and first responders should retain the flexibility to purchase from any vendor at their discretion if events preclude even simplified qualification processes.

7. Government should establish more effective vendor selection mechanisms. Price may not be the first determinant in a crisis; availability and delivery window may take precedence. It is important, therefore, that the purchaser have access to the widest range of goods and services possible. Therefore, if pre-certified or otherwise qualified vendors cannot meet the requirements, procedures should not preclude making other sources available to the purchaser.

   a. This system must, however, be open, transparent and self-auditing in the interest of integrity and fairness.

   b. At the same time, privacy protections must be incorporated into the system to ensure that participating vendors cannot access competitor information through this process.

8. Vendors should list their disaster-related inventory positions or build-up on state (or regional) registries. The number of potential disaster-related products is large, with a very dynamic fluctuation in what is in-stock. So it is probably advisable to limit registry to just those items expected to be in short supply. Additionally, this approach does not address the "deconfliction" of competing requests for the same stock. For example, a state or city may request all of a given product in stock. In the end, businesses will decide how to distribute stock within their own systems. With accurate registries, however, government will have better insight into where resources are available.

9. In addition to pre-registering items expected to be in short supply, states and regions should implement "reverse auction" systems, in which the public sector list its needs and invites private sector bids. FEMA is in the process of developing this capability for its own use. GSA vendors could respond to these orders, and those not filled by pre-qualified

vendors would be sent to the "open market" for others to fill. The price would be the one established in recommendation 2 above.

B. Revising Deficient Donations Management Systems

In a disaster, experience shows that volunteerism and pro bono donations on behalf of the private sector—businesses, non-governmental and charitable organizations combined—are the norm. The challenge for government and the private sector is to ensure that donated goods and services from the latter support, rather than interfere with, efficient public response and recovery. Many public-sector entities prefer not to deal with private donations because they add to the complexity of and often duplicate the public response mechanism.

Dismissing private-sector donations is not a realistic or necessarily desirable goal, however. Moreover, the real impediment generally is a lack of government capability to match its needs with what the private sector has and is willing to donate. That shortcoming can and must be rectified if for no other reason than to allow the government to better plan for using the full range of resources that can be made available.

"We had a number of people donating things to New Orleans. There's no mechanism in place to coordinate those things. You want to have a real transparent process in place, but you also want to utilize the gifts that are being offered."
– Dickie Brennan, Managing Partner, Dickie Brennan & Company

It is not this Task Force's intent to prescribe how non-governmental (NGOs) or charitable organizations should factor into a crisis response, except to note that they will play a major role and must be integrated along with business into the nation's response mechanisms (as the American Red Cross [ARC], as a special case, long has been).

As an example, an organization known as Aidmatrix (www.aidmatrix.org) has been working since 2000 to build global relief networks connecting people in need to surplus products and goods. It claims links with over 35,000 charitable organizations worldwide. FEMA is working with Aidmatrix to leverage their resources to respond to future US domestic disasters.

The key is to get in front of volunteerism from business and the NGO community in advance of a crisis so that those groups become effective partners and not unwanted guests.

Recommendation:

B. Improve planning, forecasting and use of assets and volunteers that businesses, NGOs and charitable organizations make available on a pro bono basis.

   1. State operations centers should add representatives from a few key NGO and charity groups to participate in planning, exercising and operations. (Businesses would coordinate donations through the Business Operations Center [BOC] concept described in Chapter 1.)

   2. FEMA should, as part of the modeling effort described in Recommendation A, improve forecasts for the most likely charitable needs for a range of scenarios, to allow the various NGOs to plan their own responses in advance of need.

3. State (or regional) registries should be created for pro bono resources not normally for sale, like warehouse space, buses, or volunteers. Such registries should include both business and NGO/charitable organization resources. They should be combined with the for-sale registries described in A.8 above.

4. A reverse auction capability attached to the system described above can also be applied to unanticipated needs for pro bono goods and services. This area is ideal for management by a council of key NGOs. However, it should be integrated and not separate from the mechanisms established for governmental and private-sector response.

5. State coordinators representing charitable and NGO organizations should work within their respective national infrastructure to fully utilize their organizations for tasks like sorting and storage, rather than pushing these burdensome tasks on to people in the affected area. They also should develop their own operating plans at the state level. Questions of storage facilities, logistics, housing, and so forth should be addressed in advance.

6. DHS should develop nationwide education programs for the private sector on how best to prepare its people for volunteer efforts—like dispensing of medications—giving them required training, inoculations, and other preparatory skills.

"You have the most phenomenal logistics network in the United States that exists anywhere in this world. Why in the world does the government insist on trying to replicate that at a much higher cost [knowing] they couldn't anticipate where the need is?"
– Ken Senser, Senior Vice President, Global Security, Aviaton and Travel, Wal-Mart Stores, Inc.

C. Logistics Processes

Throughout this report, the underlying stipulation has been that the private sector operates efficient, resilient supply chains that cannot and should not be duplicated by the government. However, there are ways that the private sector, working with government, can improve the functioning of these logistics processes in a crisis.

If, as recommended in Chapter 1, the full integration of the private sector into EOC operations at all governmental levels is achieved, it will overcome the major coordination obstacle: determining how government and business gather information, communicate, analyze problems, propose solutions, deconflict and make decisions. That is why the EOC/BOC partnership described earlier is so central to the success of the action plan described in this report. What remains is improving the "rules of the road" in effect during crisis response, thus clearing the way for the private sector to operate its supply chains effectively.

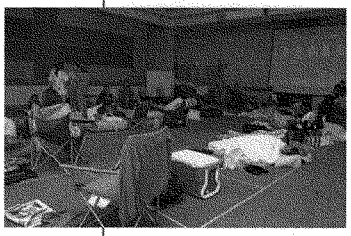
Businesses, working with government, can improve the effectiveness of logistics processes during a disaster. Here are some considerations:

Preparedness. To ease the strain on the supply chain in advance of and during a crisis, businesses need to educate their employees on emergency preparedness and encourage them to stockpile certain goods. Government also plays a role in educating the public-at-large on the need to prepare. Such preparedness can lessen peak demand during the first 72 hours of a

crisis, which may be the time required to get the supply chain back into full operation.

Business closure. In disasters that come with some pre-warning (e.g., a hurricane), state emergency officials must weigh public safety against the need to keep major supply-chain retailers open as long as possible to provide customers with emergency services and supplies. Shutting down prematurely impedes the ability of a retailer's customers to prepare their own homes and businesses for an impending crisis. It also affects retailers' ability to protect stock and employees if the notice to shut down is immediate. Here, as in other areas involving prudential judgment, reasonable balances must be struck.

Credentialing. A major effort also must be mounted to address the permitting and credentialing process imposed by public authorities in the aftermath of a crisis. In the Katrina disaster, nearly all businesses reported this shortcoming as a major impediment to restoring business continuity of community. The first issue is resolving the restrictions on professionals licensed in one state from practicing in another. The second is granting access into a disaster area for Critical Infrastructure and Key Resources (CI/KR) owners and businesses to inspect, repair and re-establish their services. The government has made headway in the second area, but both remain key prerequisites if the professional and private sectors are to quickly resume operations.



Point-of-delivery. Conceptually simple but practically demanding "last mile logistics," otherwise known as point-of-delivery issues, also must be resolved. Commercial supply chains do not possess company-controlled offload and distribution capabilities aside from those associated with their own fixed facilities. Such capabilities therefore must be provided by recipients, and since the ability to do this is by no means easily assured in most crises, it must be planned. Finally, business-owned or chartered transport should not be used to warehouse emergency supplies because the efficiency of the supply chain hinges on keeping these transportation assets in motion.

The Task Force believes that involving the private sector in the planning, exercising and execution of local, state and regional emergency response plans can identify and solve these current shortcomings in crisis-response logistics processes. If the private sector is not integrated in the planning process, we believe that government will make the same mistakes repeatedly.

Recommendation:

C. Improve the management by federal, state and local governments of business emergency response resources to maximize speed and utility and minimize redundancy.

1. Test, validate and use the EOC, BOC and BEMAC models described above to minimize physical and regulatory roadblocks and help facilitate the operation of business supply chains.

a. The proliferation of EOCs and BOCs recommended here may overburden the trained emergency response personnel available to individual private-sector organizations. A virtual presence can overcome the need to staff the BOCs 24/7. Also, periodically rotating the businesses supplying personnel to the BOC can ease the burden.

b. Plans must include a physical back-up in the event of communications or other data-sharing disruptions.

2. In order to lessen peak demand during a crisis, employers should be encouraged to develop programs that help their employees stockpile personal emergency supplies. The additional benefit is that it frees the employee to return to work sooner.

3. Improvements to the permitting and credentialing process must continue. States, working with appropriate local authorities, must create agreed standards and protocols. These procedures must be communicated to and practiced with private-sector supply chain operators.

4. For GSA-qualified companies, and others as the state crisis teams see fit, develop a system of pre-certification of the transportation fleet so that supply chains can be restarted as soon after the event as possible and can flow as freely as is practical.

5. Transfer capability to the BOC for members of state departments of transportation, law enforcement, and the private sector to coordinate movement of business-owned vehicles with critical supplies into impacted areas as efficiently as possible. This capability already exists in many state EOCs, but it needs to be applied consistently and properly on a statewide basis and should be a function of the BOC.

6. The transportation command-and-control model adopted should be consistent across states; current differences often obstruct seamless end-to-end supply chain operation when multiple jurisdictions are transited.

7. Local, state and regional authorities must take responsibility for "last mile logistics," which will then allow the private-sector supply chains to play to their strengths in responsiveness and agility.

8. Businesses should take the lead in educating local, state and regional entities on private-sector surge/supply chain management best practices to ensure they are not forced to operate inefficiently and, therefore, ultimately at greater cost to government.

Chapter 3. Legal & Regulatory Environment

Finding: Business requires a predictable legal regime to operate efficiently in an emergency situation, whether that business is engaged in charitable or profit-motivated activities. The current legal and regulatory environment is conducive to neither predictability nor efficiency.

Consistent with this finding, the Task Force recommends that Congress:

A. Enact a nationwide body of "disaster law";
B. Modify the Stafford Act to include the private sector; and
C. Hold hearings to determine which Task Force recommendations can be implemented under existing law and which require new legislation.

Action by Congress and the Executive Branch is essential for putting into place a legal and regulatory environment in which the private sector can become a full partner in the national response to disasters. We can and must ensure that federal, state and local emergency planners include the private sector in the preparations, testing, training, and execution of their responsibilities. We also must rethink the not-inconsequential issue of the legal allocation of risk through the civil justice system, most importantly tort law, as well as through regulation.

The Task Force understands that a comprehensive review of the legal and regulatory environment surrounding emergency response will require considerable time and effort, and we urge Congress to schedule hearings to deal with longer-term issues. But we also urge government to concentrate initially on specific short-term objectives so that an adequate private-sector response is available for the next disaster—not one that may befall us years from now.

One example of an important short-term action would be to implement the critical EOC/BOC partnership concept discussed earlier. That action could be done through a mandate to DHS under existing law, even as other long-term legislative solutions are being considered.

Another important action would be to adopt immediate legislative fixes to the Stafford Act (such as those included in "The Post-Katrina Emergency Management Reform Act of 2006" [S. 3721], introduced by Senator Susan Collins on July 25, 2006).

A National Disaster Law

Major disasters are a national issue, and uniformity of law across states is essential to the efficient leveraging of the nation's business assets in dealing with them. During the Katrina response effort, many out-of-state businesses that tried to help had little or no familiarity with the laws of Louisiana, which hurt their efforts and hurt the people of New Orleans. While we must respect the purposes and value of federalism, we should nevertheless explore whether we need a body of federal disaster law to preempt the heterogeneous patchwork of state law in this particular context.

"Business normally conducts [its] activities in an environment which is governed by civil authority and provided access to resources through the commercial marketplace. In a disaster where civil authority is overwhelmed and normal commercial activity disrupted, assistance at the federal level may be necessary in order for private sector entities to perform expected disaster response functions."
– Duane Ackerman, President & CEO, BellSouth Corporation

Two basic principles should guide us in thinking about such a body of law:

- Things should get easier, not harder, and better, not worse, during a local/regional disaster or incident of national significance.
- Individuals and businesses acting in good faith should be able to confidently provide assistance based on a predictable set of rules and responsibilities governing their conduct.

Following the hurricanes of 2005, a great number of laws and regulations necessarily were waived, suspended or modified—HIPAA (Health Insurance Portability and Accountability Act) privacy provisions being a case in point. This body of waiver authority should be kept "on the shelf" for consideration in future disasters. However, to be effective when invoked, government must communicate with the private sector in advance of and during the crisis to set a level of expectations sufficiently high so that the predictability standard is met.

Recommendation:

A. Congress should hold hearings and produce legislation for a nationwide body of "Disaster Law."

1. Considerations for such legislation are: 1) lack of predictability, 2) differences between laws applicable to pre-disaster agreements and those applicable to people and organizations who deliver goods and services voluntarily after a disaster occurs, and 3) variations in state law.

   a. With respect to liability, Congress should improve protections with the aim of ensuring predictability of liability for private-sector entities and citizens providing Good Samaritan (no reimbursement to the provider) goods and services, <u>particularly when those goods and services are specifically requested by the government, e.g., FEMA or a state or local government:</u>

      1. Safe harbor provisions in existing law should be reviewed and cataloged in a Stafford Act provision (see Recommendation B below);

      2. Good Samaritan activities deemed appropriate to federal protection but not covered in current law should be identified.

2. Congress should clarify and standardize to the extent possible the liability of professionals acting in good faith during disasters.

   a. Examine the need for government-backed secondary insurance, or some other type of indemnification mechanism (perhaps analogous to the Federal Deposit Insurance Corporation [FDIC]), to mitigate some of the potential private-sector risk in emergency response situations.

   b. Investigate the effect of federal law, regulations and standards for disaster response on the liability insurance coverage to businesses.

c. Review federal laws, regulations and standards regarding medical response to disasters to determine where revisions can improve the effectiveness, safety and efficiency of medical care delivery and the protection of medical facilities and professionals in those circumstances. For example:

1. Triage: The Department of Health and Human Services (HHS) could set triage standards to be used as the benchmark in determining negligence by health care providers dealing with mass casualties and by emergency medical responders to disaster scenes. HHS currently provides only voluntary triage standards and supporting tools. Moreover, many different triage systems are in use nationwide, setting up the certainty of problems when medical augmentation teams from outside a disaster area support a local triage system different than the one in which they are trained.

2. Lack of Adequate Vaccines and Medicines: Protection for healthcare providers needs to be established in case a scarcity of effective vaccines and other medicines early in a crisis requires experimental and out-of-formulary treatments.

3. Transportation of Patients in Non-Standard Vehicles: Protection needs to be established for medical facilities and transportation providers who through necessity use emergency vehicles not normally suitable to the purpose for transporting injured or sick persons.

d. To the maximum extent possible, facilitate ordinary rules of risk and liability allocation being applied to emergency situations.

e. Provide for a predictable, single (and probably federal) jurisdiction for hearing disputes arising in the course of response to an Incident of National Significance.

3. With regard to regulation, federal agencies with oversight/regulatory authority over the private sector need to clarify and promulgate procedures that allow the agencies to quickly implement discretionary authorities for the relaxation of regulations in the event of an emergency. These authorities need to be pre-packaged as much as possible so that they can be triggered by an appropriate declaration of emergency. Examples include:

a. Antitrust: DHS should take advantage of the "voluntary agreements" section of the Defense Production Act, PL 81-774, which allows competitors (with government notice and clearance) to allocate certain resources.

b. Effects on the Environment: The entire body of environmental impact laws and regulations can usefully be reviewed to determine if standard waivers need to be developed to cover disaster situations.

c. Licensing: Develop uniform rules concerning interstate recognition of business and professional licensing during times of emergency,

"Some agencies like the Department of Education get very high marks, but one problem was that the agencies did not seem to speak with one another. While we had FEMA and others at one door helping us to re-open, we had the immigration service at another talking about deporting our foreign students because they weren't in school. These were regulations that could have been suspended given the situation."
- Yvette M. Jones, Chief Operating Officer and Senior Vice President for External Affairs, Tulane University

perhaps incorporating a trigger mechanism activated by the Governor of the state where the emergency situation exists.

d. Privacy: Rules governing the release of personal data by competent authority during a crisis should be reviewed and clarified. During Katrina, much confusion and concern was generated because of statutes (such as HIPAA) that appeared to prohibit the release of personal data.

e. Service delivery: We must review and if necessary revise laws and policies concerning how and when providers of goods and services during a catastrophe can terminate service after a crisis has passed—especially laws that would affect providers of free or discounted goods. Companies providing services such as medical care or housing after Katrina found that they could not terminate services once a patient/tenant was in the system, even if that patient/tenant abused or violated the terms of service.

f. Trade restrictions: Review the Trade Agreement Act (19 USC 2501, *et seq.*) and the Buy America Act (41 USC 10a - 10d) to determine if waiver authority is warranted to ensure these laws do not restrict government's purchasing from non-domestic sources in an emergency.

g. Regulatory agencies should establish and test contact procedures and empower federal regulators to respond quickly to private sector requests for regulatory relief when a crisis has occurred.

"People need cash. Law enforcement needs to...partner up with the banks so that as branches are opened without power, you're not putting employees at risk. [T]hey (law enforcement) think it's a business thing: 'I'm not going to help you at Bank United.' [But]our service is essential to the community, and if I [open] a branch without any alarm, without any cameras, and you're looking at $80,000 in your teller drawer, and you've got a line of people, you're not going to feel too good."
– Ramiro Ortiz, Chief Operating Officer, BankUnited Financial Corp.

B. Revise the Stafford Act

The Robert T. Stafford Disaster Relief and Emergency Assistance Act (Stafford Act), 42 USC 5121-5206, is a federal law designed to bring an orderly and systematic means of federal natural disaster assistance to state and local governments in carrying out their responsibilities to aid citizens. The Stafford Act is a 1988 amended version of the Disaster Relief Act of 1974, Public Law 93-288. The amended act created the system in place today by which a Presidential Disaster Declaration of an emergency triggers financial and physical assistance through FEMA. The Act gives FEMA the responsibility for coordinating government-wide relief efforts and includes the contributions of 28 federal agencies and non-governmental organizations, such as the American Red Cross. In October 2000, Congress amended the law with passage of the Disaster Mitigation Act of 2000, Public Law 106-390, which permitted contributions of federal resources to private nonprofit entities under certain conditions.

The SAFE Port Act of 2006 (PL 109-347, Sect. 607) extends the Stafford Act to include the private sector, but only to the extent that it precludes the head of a federal agency from denying or impeding essential service providers[12] access to the disaster site or impeding them from performing restoration or repair services.

[12] Essential Service Providers include entities that provide telecommunications, electrical power, natural gas, water and sewer services or any other essential services as determined by the President. They include municipal, nonprofit and private, for profit, entities in the act of responding to an emergency or major disaster.

Several recent congressional actions have proposed changing the Stafford Act yet again, but none of these efforts have been successful. The Task Force believes that Congress should extend coverage of the Act beyond state and local government to include the private sector, with particular attention to the provision of security or protection of private-sector personnel and assets operating in a disaster zone. Authorities should be automatic upon presidential declaration of a national disaster, but protections offered should be specific and limited to situations where it is impractical or impossible for the private sector to provide for its own security.

Recommendation:

B. Congress should revise the Stafford Act to designate the private sector as a critical component of a comprehensive disaster response mechanism.

1. Such provision in law can usefully support designated categories of private-sector partners:

   a. To participate as full partners in the planning, training, equipping, certification, exercise and execution of disaster response;

   b. To be afforded federal assistance when necessary to carry out disaster responsibilities, e.g., providing escort and security so that emergency repairs, etc., can be effected in a disaster zone;

   c. To coordinate and request assistance directly through the appropriate federal agency (such as designated Source Selection Authorities [SSAs] and NRP-designated lead agencies) without having to work through third-party (i.e., FEMA) officials.

C. Congressional Hearings

While remedies to the private sector's full participation in the nation's disaster response capabilities are urgent, such remedies should not be taken hastily. Adequate consideration and deliberation before deciding to legislate is in order—once in place, law is hard to undo. The Task Force therefore urges Congress to review carefully the body of existing law pertaining to disaster response and the agencies of government responsible for carrying out that law. The initial focus of its investigation should be to determine which of the recommendations of this Task Force can be implemented under existing statute, and which require new legislation.

A series of hearings, early in the 110th Congress, can build momentum for systematically integrating the private sector and its resources into the national response to disaster in the near term, even as longer-term new legislation is being crafted.

Recommendation:

C. Congress, early in its 110th session, should hold hearings to determine which remedies suggested by this Task Force can be implemented under existing law and authority, and which may require new legislation.

Chapter 4. An Expert's Guide to Priorities and Sequencing for the Integration of the Private Sector into U.S. National Disaster Response Planning and Execution

Government should move quickly to integrate business into its disaster response planning, doctrine, exercises and operations and ensure that adequate resources are devoted to implementing Task Force recommendations at the state and regional level on a sustainable basis.

The recently released National Infrastructure Protection Plan (NIPP) acknowledges that Critical Infrastructure and Key Resources (CI/KR) are essential to the nation's security, public health and safety, economic viability, and way of life. Natural or man-made disasters that weaken or destroy CI/KR will significantly disrupt the functioning of government and business alike, producing cascading effects far beyond the targeted infrastructure and physical location of the incident. Direct attacks, natural disasters or technological hazards could produce catastrophic losses and will require the coordinated collaboration of the whole of society—public and private sectors—to put the country back on its feet.

"You want to re-center from a government-dominated, marginally assisted system to a genuinely collaborative partnership, because in fact the private sector brings more speed and more resources and more capability than government has internally."
– Newt Gingrich, former Speaker of the U.S. House of Representatives

The Business Response Task Force recommendations proposed in this report are directed toward creating mechanisms that would integrate the full capabilities of the private sector as a critical component of a comprehensive national disaster response. This chapter addresses the priorities and sequencing necessary to put those steps into action.

Federal Plans and the Private Sector

The federal government, through DHS, has done a good job developing the policy frameworks to be used in all aspects of protection and disaster management. The National Response Plan (NRP), National Incident Management System (NIMS) and the NIPP together provide for a comprehensive approach to ensuring the viability of the national community from a structural and policy perspective. What is still missing, however, are the operational components and mechanisms that allow all members of the community to participate as required to fulfill the objectives of the risk management framework described in the NIPP.

DHS' risk management framework addresses economic sectors in a vertical fashion, but in real economies businesses operate within a community, not an industrial sector. Communities are not only customers; they also make decisions that affect businesses' ability to function. Likewise, communities cannot return to normal function without the private sector, which owns or operates 85 percent of U.S. critical infrastructure. Figuring out how to reconcile the top-down federal sectoral view with the bottom-up community-centered perspective of business means that determining where the private sector should plug into federal doctrine is a complex but vital undertaking.

While that process plays out—as it must—we must do what we can on other fronts, and the actual community level is the best place to start.

The Near Term

The Task Force recommends that the near-term focus be centered on implementing the Business Operations Center (BOC) concept described in Chapter 1. The EOC/BOC partnership model provides the operating processes necessary for private sector-involvement in the risk management framework, focused initially on immediate response. The BOC provides a basis for public-private collaboration that creates the necessary level of trust needed for full integration of the private sector to succeed. This is most easily achieved at the state and local levels because, in most cases, such relationships already exist organically as part of normal social life—it's "the community thing."

Does that mean that we have to create 55 separate BOCs, one for each state, federal jurisdiction and territory? Ideally, yes; but achieving this goal will depend on the political and business leadership at the state level. The same is true for BOCs in major urban areas. New York City and Los Angeles County are creating their own versions, and others should follow.

There also is a question of resources. In the end, it is hard to see any other way to proceed than to have some federal dollars, through some combination of grants, credits or offsets, or by direct appropriation, support the EOC/BOC concept.

A private-sector presence also should exist at the regional level. The June 2006 DHS Nationwide Plan Review Phase 2 Report suggests that a new DHS-directed regional system is needed.[13] Were such a capability developed, the inclusion of a BOC would be an important component. Establishing BOCs in each of the ten current FEMA regions would at least be a good start.

The creation of state and major metropolitan area BOCs should be put on the fast track for— deployment, training and exercising before the end of 2007. Regional BOCs will follow on the success of deployment at the state/major metropolitan area levels.

The Horizon

Doctrine development. The longer-term objective is to formalize private-sector participation in the National Response Plan and other doctrine. Ultimately, the private sector needs a permanent presence at the regional and federal doctrinal development level. Task Force members are participating in the current revisions of the NRP and NIMS and will seek to codify the public-private partnership collaborations recommended in this report.

Capabilities-based resource planning. To begin, the private sector needs to have a large role in the current development/revision of the Universal Task List (UTL) and Target Capabilities List (TCL). The UTL and TCL were developed at the direction of *Homeland Security Presidential Directive(HSPD) 8: National Preparedness* with the participation of federal,

[13] U.S. Department of Homeland Security, *Nationwide Plan Review: Phase 2 Report*, June 16, 2006.

state and local government representatives and professional associations representing government responders. The TCL provides the basis for preparedness for all of the national planning scenarios and each of the major missions of prevention, protection, response and recovery.

The TCL tiering summary chart assigns capabilities, outcomes, capability resources, and roles to government, non-governmental organizations, the private sector, and citizens. On cursory review, the Task Force believes the private sector can make major contributions in the planning, management and support of at least the 25 of the current 37 target capabilities in the TCL. Further, we believe that the current tiering summary chart under-represents the contributions the private sector can make to national preparedness, thereby both raising the cost of public-sector investment in such capabilities and reducing the effectiveness and efficiency of preparedness efforts.

The development and maintenance of TCL capabilities by federal, state and local governments is supported by congressional appropriation. Where capabilities are assigned to the private sector in the TCL, government could likewise support the development and maintenance of such capabilities in federal equipment, training, certification, credentialing and exercise programs.

Another area for private-sector inclusion is in the development and implementation of changes to the National Incident Management System (NIMS). The NIMS reflects the doctrine contained in *HSPD 5: Management of Domestic Incidents*. Of the three NIMS components, only the Incident Command System (ICS) is defined and, as yet, does not clearly indicate where or how the private sector plays in its execution.

Likewise, as the other two components of NIMS are defined (the Multi-agency Coordination System [MACS], which describes the relationships among the operations centers at all levels, and the Public Information System [PIS]), inviting early private-sector participation will ensure that its views are reflected in the final products. Moreover, creating an enterprise architecture for the NIMS will complete the development cycle by defining public- and private-sector concepts of operations, organizational relationships, activities, information needs, rules and supporting systems. DHS may want to consider separate development of an enterprise architecture to support the NRP.

Similarly, federal agencies should coordinate with those private-sector entities governed by the National Infrastructure Protection Plan (NIPP) and its sector-specific supporting plans to develop a process and schedule for affected private-sector entities to come into compliance with those plans.

Operations planning. In the case of operations planning, DHS Secretary Michael Chertoff has told Congress that the system is broken and cannot be fixed without a major investment. A new National Planning System (NPS) for coordinated federal, state, tribal, local and NGO/private-sector planning has not yet been authorized or funded. This is a clear opportunity to get the legislation right the first time relative to private-sector participation. In the meantime, the private sector needs to make its voice heard on Capitol Hill to give substance to a requirement for private-sector participation that is currently defined only in the broadest terms.

In addition to establishing private-sector participation in planning at the national level, the NPS should carve out room for business-to-business efforts. Many areas of response and recovery are most effectively and efficiently organized and implemented by the affected private sector, not as a government-controlled activity. An excellent example is the mutual aid pacts in place among the utility companies in the southeastern United States. The planning system should be sensitive to and try to identify areas of the economy that are best restored by the private sector itself in the event of a disaster. In doing so, government should encourage and support processes by which industry groups can organize and plan—and publish those plans as part of the NPS.

Having the private sector commit resources and aggressively pursue ongoing participation in thousands of local, state and federal contingency planning efforts will never be fully achievable. But inclusion of the private sector in the NPS can probably be accomplished at the federal and state levels, in the largest urban areas—and at the regional level. The business case for doing this planning is the basis for this report, and it is, to the Task Force, compelling.

Training and exercises. As stated repeatedly in this report, repetitive, detailed training and exercising of the plans developed for public-private collaboration are essential for such operations to work efficiently in an actual disaster. Some members of the Task Force feel that a major national exercise that truly strains the system must occur in the near term if we are to honestly confront the shortfalls and unknowns that exist in our current plans. To encourage public-private collaboration, DHS grant funding to the states and other entities must be contingent on demonstration of significant participation by the private sector in disaster training and exercises.

Operations. Based on the successful outcome of private-sector and government collaboration on implementing the recommendations in this report, in an actual disaster the private sector would be able to carry out the roles it had equipped itself for based on capabilities-based planning, defined in doctrine, planned in contingency and crisis action plans, and trained for in exercises.

Lessons-learned assessments. The operations continuum is not a circle but a never-ending spiral. The impetus for change in doctrine and operations is the assessment program. The private sector must play its role here as well. As a consequence of scale, the most extensive and expensive commitment required is at the local and state levels. Once again resources for this activity must come from federal, state and private coffers.

"Congress can and should encourage DHS to provide grant funding to implement the recommendations of this report. Without strong Congressional action, public-private collaboration in crisis management and response will remain an afterthought."
– Former Sen. John Breaux (D-LA)

Resourcing Private-Public Collaborative Relationships

Finding the resources to implement the recommendations in this report will be difficult but doable if we proceed gradually from what now exists to the achievement of the ideal. As reported here, many examples of state EOCs exist. In a few, the BOC concept has been implemented. As the concept scales up to the regional or federal level, new sources of funding will have to be identified.

Along the operations continuum, doctrine development, capabilities-based planning, and operations planning require an excess of brainpower over cash. The major investment is talent and time, and the Task Force believes that the private sector is willing to commit those resources if it is given its seat at the table. The true costs occur during the training, exercising, operations and assessment phases. The current grant program is geared largely to funding one-off exercises.

The Task Force urges Congress to commission DHS to begin development of an architectural framework linked to or as part of the NRP to ensure that fully functional and staffed BOCs can be maintained in each state, urban area and region.

Recommendation:

Ensure that adequate resources are devoted to implementing Task Force recommendations at the state, regional and federal level on a sustainable basis.

Appendices F through I at the end of this report identify and prioritize specific desired outcomes and policy drivers keyed to the Task Force recommendations.

Appendix A – Business Response Task Force Charter

June 2006

CHARTER

BENS Business Response Task Force: BENS has formed a Task Force to review and recommend to the U.S. Government steps to systematically integrate the capabilities of the private sector—principally that of the business community—as a critical component of a comprehensive disaster response mechanism. Membership is comprised of senior business leaders from U.S. industries closely tied to disaster response: telecommunications, supply chain logistics, utilities, real estate management, and so forth. Business leaders understand the need to ensure the continuity of their community in order to maintain their own business continuity, but business-government collaboration in major disasters is largely disorganized.

BENS: For nearly 25 years, Business Executives for National Security has served as the primary channel through which senior executives can help build a more secure America. BENS is a national, non-partisan, non-profit organization that harnesses successful business models from the private sector to help strengthen the nation's security.

Scope: We propose to collect lessons learned during the responses to Katrina, 9/11, and other incidents of national significance. We believe that the experiences, reactions, and responses to catastrophic events apply equally to other kinds of national disasters and are, therefore, appropriate exemplars for our review. The Task Force will focus on the time between when the hurricanes were first predicted to make landfall in the U.S. through the response phase of operation.

Process and final report: The Task Force will analyze lessons from these disasters to recommend reforms enabling future improved public-private collaboration and coordination. The Task Force will provide examples of response functions for which it makes sense to rely on the private sector, and will offer policy recommendations to optimize the contributions of business during national disasters. It will propose a program leading to an architectural framework to integrate private sector participation into disaster response at all levels—local, state, and regional—and under the execution of the National Response Plan.

Timing: The Task Force intends to complete work within approximately 45 days from the start date.

Appendix B – Task Force Members, Advisors and Staff

Task Force

F. Duane Ackerman (Chairman)
President and CEO
BellSouth Corporation

The Honorable John Breaux (Co-chair)
Senior Counsel
Patton Boggs LLP

The Honorable Newt Gingrich (Co-chair)
The Gingrich Group

Lawrence Babbio
Vice Chairman and President
Verizon Communications, Inc.

General Charles G. Boyd, USAF (Ret.) (Ex Officio)
President & CEO
Business Executives for National Security

Guy F. Budinscak
Atlanta Managing Partner and
Regional Managing Partner, Strategic Clients
Deloitte & Touche LLP

The Honorable Sidney Harman
Executive Chairman
Harman International Industries

Christopher C. Melton
Managing Director
The White Oak Group, Inc.

Robert Nardelli
Chairman, President and CEO
The Home Depot, Inc.

David Ratcliffe
Chairman and CEO
Southern Company

William J. Rouhana, Jr.
Managing Member
WS Management, LLC

Roger Staubach
Chairman and CEO
Staubach Companies

Paul G. Stern
Chairman
Claris Capital, LLC

Advisors

Richard Andrews, Ph.D.
The National Center for Crisis and
Continuity Coordination

Anthony D. Begando
Chief Executive Officer
Tenon Consulting Solutions, Inc.

Peter Carpenter
Founder, Mission and Values Institute

Steve Carpenter
Director, Customer Service and Support
DataPath, Inc.

Dr. Scott S. Cowen, Ph.D.
President
Tulane University

Cherie Curry
Stock Plan and Communications Manager
Harman International Industries

General Ralph E. Eberhart, USAF (Ret.)
President and CEO
AFBA

Steven Cash
Principal/Counsel
PRTM

Tom Fricke
Vice President Asset Protection
The Home Depot, Inc.

Rahul Gupta
Director
PRTM

William I. Hancock
Fellow, Integrative Center for Homeland Security
The Bush School of Government and Public Service
Texas A&M University

Scott Hefter
Director, Government Sector Lead
PRTM

Mike Hickey
Vice President
Government Affairs, National Security Policy
Verizon Communications Inc.

Frank W. Jenkins
Senior Vice President
Science Applications International Corporation

Charles Lathram
VP Security and Business Control
BellSouth Corporation

Appendix B – Task Force Members, Advisors and Staff (cont'd)

Thomas Lee
Director, Business Development
Monogram Systems

Admiral James M. Loy, USCG (Ret.)
Senior Counselor
The Cohen Group

William G. Raisch
Director
International Center for Enterprise Preparedness (InterCEP)
New York University

Michael Sherberger
Former Director, Georgia Office of Homeland Security/
Georgia Emergency Management Agency

Ken Senser
Sr. Vice President - Global Security, Aviation & Travel
Wal-Mart Stores, Inc.

Brian Spickard
Director, Business Assurance
Southern Company

Lacy Suiter
Director of Executive Education Programs
Center for Homeland Defense and Security
Naval Postgraduate School

Scott Louis Weber
Patton Boggs LLP

Staff

Business Executives for National Security

Lauren Armistead
Deputy Director, Homeland Security Advisory Council

Ken Beeks
Vice President, Policy

Ern Blackwelder
Sr. Vice President, National Business Force

Jason Blake
Intern

Laura Bondesen
Intern

Colin Bucher
Policy Analyst

Joe Byrne
Director, Homeland Security Advisory Council

Conrad H. Busch, Jr.
Director, Metro Atlanta

Danielle D. Camner
Director of Policy

Michael Doubleday
Sr. Vice President, Policy

Anne Ferris
Regional Director, California

Walter Gramm
Executive Director
New Jersey Business Force

David Guthrie
Director
Mid-America Business Force

Don Hays
Chief Operating Officer

Travis Hill
Intern

Lynne Kidder
Vice President
National Business Force

William F. Lawson, III
Director, Kansas City

Clinton E. Long
Director for Publications/Web

Melita Leoussis
Intern

Linda Moseley
Executive Asst. to the President & CEO

Peter Ohtaki
Director
Bay Area Business Force

Paul Taibl
Vice President, Policy

Kiersten Todt Coon
Vice President, Policy

John H. H. Turner, III
Director/Program Manager
Georgia Business Force

Science Applications International Corporation (SAIC)

Lindsey E. Arnold
Program Manager

M. Wendy Reid
Senior Analyst

Pat A. "Doc" Pentland
Program Manager

James C. Sherlock
Program Development Manager

Julie C. Simpson
Policy Analyst

Donald C. Snedeker
Senior Analyst

Kenneth B. Van Dillen
Project Lead

Editor

Adam Garfinkle

Paul Taibl

Appendix C – List of Survey Interviews

Admiral Jim Loy, USCG (Ret.)
ALZA Corporation
Armed Forces Benefits Association
AutoNation, Inc.
Avatar Holdings Inc.
BankUnited Financial Corp.
Baptist Health South Florida
BellSouth Corporation
The Biloxi Sun Herald
Boh Bros. Construction Co., LLC
Burger King Holdings, Inc.
CACI International Inc
Cargill, Incorporated
Chevron Corporation
Cisco Systems Inc.
Citigroup Inc.
City National Bank
Coca-Cola Enterprises Inc.
Colonial Pipeline Company
ConAgra Foods, Inc.
Cushman & Wakefield Inc.
Darden Restaurants, Inc.
DataPath, Inc.
Deloitte & Touche LLP
Deutsche Bank AG
Dickie Brennan & Company
D.J.'s National Food Service
The Dow Chemical Company
Dr. Kathleen E. Toomey, M.D., M.P.H.
Durr Heavy Construction, LLC
Exponent, Inc.
FedEx Corporation
Food Lion, LLC
Food Marketing Institute
Gene Matthews
General Electric Company
Greenberg Traurig, LLP
Harman International Industries, Incorporated
Harrah's Entertainment, Inc.
The Home Depot, Inc.
INSTEDD
Intel Corporation
International Business Machines Corporation
iWave, Inc.
J.B. Hunt Transport Services, Inc.
Johnson & Johnson
JPMorgan Chase & Co.
Keefe, Bruyette & Woods, Inc.
Kraft Foods Inc.
Lacy Suiter
Laitram L.L.C.
Lockheed Martin Corp.
The Macerich Company
Marriott International, Inc.
McKesson Corporation
Miami Herald
Michael Sherberger
Monogram Systems
NC4 (The National Center for Crisis and Continuity Coordination)

Appendix C – List of Survey Interviews (cont'd)

Ochsner Clinic Foundation
Oreck Corporation
Patton Boggs LLP
Peoples Financial Corporation
Pfizer Inc.
Raymond James Financial, Inc.
Republic Services, Inc.
Richard Andrews
Royal Caribbean Cruises Ltd.
Ryder System, Inc.
Sandler O'Neill & Partners, L.P.
Science Applications International Corporation (SAIC)
The Honorable John Breaux
Southern California Edison
Southern Company
The Honorable Newt Gingrich
St. Barnabas Health Care System
Steven Cash
Tenon Group Plc
The Staubach Company
Toll Brothers, Inc.
Tulane University
United States Northern Command
University of Miami
Verizon Communications Inc.
Wachovia Corporation
Wal-Mart Stores, Inc.
The Westfield Group
The White Oak Group, Inc.
William I. Hancock
WS Management, LLC

Appendix D – Relevant Recommendations from Federal Government After-action Reports and Other Sources

Numerous reports have reviewed the response to Hurricane Katrina. Many of these reviews, including those conducted by Congress and the White House, favor improving emergency preparedness, response, and recovery via improved partnerships with the private sector.

1. The White House report entitled *The Federal Response to Hurricane Katrina: Lessons Learned* enumerated specific recommendations to be implemented by collaboration with the private sector. The White House report recommended that private-sector organizations "actively participate in all phases of a Federal Disaster response." The **House of Representatives' report, *A Failure of Initiative,*** provided anecdotal evidence of failures in collaboration. The report of the **Senate Committee on Homeland Security and Governmental Affairs, *A Nation Still Unprepared,*** "examined in detail the actions of officials of local, state and federal government departments and agencies."

Public-Private Collaboration

The House report stated that critical elements of the National Response Plan (NRP) were unsuccessfully executed during Hurricane Katrina. Gaps in the National Communications System, a component of the NRP, resulted in miscommunication and slow response in delivering relief supplies. The report illustrated how communications inoperability led to issues with command and control and situational awareness.

Another recommendation, according to the Senate *A Nation Still Unprepared* report, is "to enhance regional operations to provide better coordination between federal agencies and the states and establish regional strike teams." Among their other duties, the regional offices should "enhance cooperation with NGOs and the private sector, and provide personnel and assets, in the form of Strike Teams, to be the federal government's first line of response to the disaster."

The White House report recommended actively engaging the private sector in reviewing the NRP and the NIMS and finalizing the Interim National Infrastructure Protection Plan. Both Congress and the White House suggested that slow delivery of relief commodities can be remedied via more robust relationships with the private sector. The report recommended that DHS mandate "pre-competed" private-sector contracts for arranging advanced communications capabilities.

Surge Capacity for Goods and Services

The House Katrina report also detailed problems with medical response, including inadequate communications equipment, confusion relating to hospital evacuations, and problems with credentialing. The report referenced failures in advanced contracting, which led to hasty acquisitions and vulnerability to fraud. One company tasked with supplying temporary housing experienced contracting issues when the requirements for the work order changed midway through their response.

The White House report specified that HHS arrange "pre-configured" teams of health care professionals, including volunteer health professionals from the private sector. DHS should partner with the private sector to develop a scalable, flexible, and transparent logistics system for the procurement and delivery of goods and services. DHS should pre-identify private-sector resources to provide disaster support. Also, states are encouraged to enter into contractual arrangements with private-sector companies for procurement and delivery of goods prior to a disaster.

Legal and Regulatory Framework

The House report cited exemplary companies with existing emergency preparedness plans. The White House suggested that DHS overhaul regional disaster plans by collaborating with the private sector and by setting standards for private-sector preparedness against which regional plans can be measured.

The White House recommended that DHS lead an interagency effort to remove federal and legal liability obstacles to utilization and coordination of private-sector resources during a disaster. Private-sector actors also are encouraged to plan their "giving streams" at the local level.

2. The DHS "Lessons Learned Information Sharing" report on public-private partnerships for emergency preparedness explains the need for coordination between public safety agencies and private sector entities. Public-private relationships must be established prior to emergencies. Familiarity of the two sectors with each other's capabilities and response procedures is paramount. The private sector plays a vital role in emergency situations; it employs most of the nation's workforce, owns 85 percent of critical infrastructure, and produces essential goods and services. The public sector often underestimates the private sector's involvement in emergency preparedness, while the private sector often overestimates the capabilities of the public sector. Collaboration by public groups with the private sector is imperative to ensure emergency preparedness and safety.

Public-Private Collaboration

Many public- and private-sector groups have established partnerships to improve emergency preparedness, prevention, mitigation, response, and recovery efforts. This allows the public- and private-sector entities to share risk, vulnerability, and threat information; coordinate response and recovery operations; develop all-hazards plans to pool resources and information; and share educational and training opportunities.

However, many communities have failed to establish such partnerships, either because they are viewed as costly and time-consuming or because the public-private relationships lack the necessary trust and understanding to exchange sensitive information and allocate valuable time and resources.

The section on developing partnerships outlines possible steps toward establishing long-lasting relationships with public-or private-sector groups. The steps include:

1. Clearly define purpose and objectives
2. Identify partners
3. Develop incentives to try to persuade potential partners to join.
4. Secure commitment, usually by developing personal relationships with individuals at the senior level and with individuals responsible for mitigation, response, and recovery operations.
5. Initiate dialogue to discuss capabilities, resources, and opportunities for mutual assistance.
6. Build the partnership by establishing objectives that reflect the interests of all members, identifying leaders, forming a plan or task force around each objective, and planning regular activities to ensure long-lasting relationships.

Surge Capacity for Goods and Services

Large-scale incidents can quickly deplete response resources, leading to a surge in demand for goods and services. Sharing resources is often prevented by questions surrounding liability, cost, and availability of resources. In order to overcome these obstacles, public-private partnerships must identify available member resources and then develop procedures to manage and share them.

According to the report, resource sharing plans should accomplish the following:

- Define how partners borrow and/or expend resources during emergencies.
- Include agreements on inventorying, requesting, allocating, using, and returning resources.

- Include qualifications that must be met in order for resource sharing to occur. Such qualifications can include:
  - prior depletion of public sector resources
  - expected impact of the incident on the private sector group's area of concern
- Hold public-private training exercises that include resource sharing plans so partners can practice requesting, locating, using, and returning resources.
- Include agreements on liability and reimbursement.
- Establish a single resource inventory for the responding agency.
- Establish resource request procedures.
- Develop rules for resource allocation, usage, and return.

Legal and Regulatory Framework

An important obstacle to public-private partnerships is the hesitancy to share sensitive or proprietary information. At the federal level, DHS has undertaken various initiatives to provide secure ways to share information. Many local communities have not taken such initiatives, and fears persist concerning improper dissemination and/or the cost of secure sharing. Private groups also occasionally lack clearances to view necessary information. In order to build partners' trust in each other's ability to protect sensitive information, the report suggests formalized information sharing networks with security features that protect and limit the dissemination of and access to sensitive information. The report also suggests assigning a single public safety agency to disseminate all threat notifications to guarantee accuracy and reliability.

The report lauded a number of Presidential Directives and national strategies that have encouraged public-private partnerships. Most such initiatives focus on establishing relationships between public and private groups on a national level and facilitating information sharing among industries and federal agencies. On a local level, however, public safety agencies and private sector groups in many communities do not collaborate effectively. DHS has established initiatives to help foster local partnerships, and other developmental programs exist in some areas through non-profit associations. Additionally, many industries face local pressure or are legally obligated to enact safety and preparedness measures that require coordination with the public sector. The report also encourages communities lacking such programs or initiatives to dedicate time and resources to establishing public-private partnerships.

3. Government Accountability Office (GAO) testimony, "Hurricane Katrina: Planning for and Management of Federal Disaster and Recovery Contracts," April 10, 2006, contains many cogent observations about what went right and what went wrong.

Public-Private Collaboration

Government contracts have long been a mainstay in public-private enterprise, but they now face new challenges. In the face of unexpected contingency scenarios, an adequate response is of paramount importance, but efficiency and avoiding waste cannot be overlooked. Contracts were inked hastily and oversight was lacking, as there was an insufficient number of trained personnel to conduct uversight, as well as unclear definitions and delegations of responsibility. The agencies scrutinized by this report–FEMA, GSA, and the U.S. Army Corps of Engineers–have high-risk acquisition practices that equate to a "vulnerability to fraud, waste, and abuse." The efficiency owed to taxpayer dollars can be better facilitated with advanced planning and pre-arranged contracts.

Surge Capacity for Goods and Services

A lack of communication between agencies at the federal level and between levels of government, as well as a failure to anticipate needs, led to the inefficient acquisition and allocation of goods and services. Specifically, the need for temporary housing was underestimated, and for other goods and services that

were anticipated, the mechanisms by which to acquire them, legal and logistical, were neither fully understood nor well lubricated. Furthermore, the GAO report notes tensions in upholding Stafford Act preferences to engage contracts with businesses in the affected area (e.g., contracting with Gulf region business in recovering from Hurricane Katrina). The difficulty of taking the initiative to engage local businesses instead of falling back on national contractors, coupled with the fact that there was vast confusion among GSA and FEMA officials about the actual Stafford Act preferences and how to apply them, resulted in local businesses often being overlooked in taking advantage of government contracting opportunities. GSA officials state that they plan to review the Federal Acquisition Regulation (FAR) to clarify Stafford Act guidance.

Legal and Regulatory Framework

Along with Stafford Act implications and oversight complications, other legal and regulatory issues were factors in the response to Hurricane Katrina. The Army Corps of Engineers noted a hindrance to pre-arranged contracts in that funding must be secured for a particular mission before formal preparation can ensue. Regarding communication and continuity, especially in contract oversight, turnover and transition can pose problems, and the Corps disclosed its policy to rotate personnel every 29 days to minimize costs due to regulations under the Fair Labor Standards Act. To combat these problems, FEMA stated that it is implementing a process to better distribute work and information among rotating personnel, and GSA is investigating alternative options for smoother contract oversight.

4. The Council on Foreign Relations (CFR) Report, "Neglected Defense: Mobilizing the Private Sector to Support Homeland Security" by Stephen Flynn and Daniel B. Prieto, March 13, 2006, offers ten clear recommendations.

Public Private Collaboration

- Change policy paradigm from telling companies to protect themselves to offering leadership in securing critical infrastructure.
  - Current attitude is that the there are enough market incentives for the private market to provide levels of security commensurate with the threat of catastrophic incidents–but this is untrue. The government must take an active role understand how the private sector operates and then use this understanding to encourage the private sector to provide more security.

- Create a national list of priorities, as mandated by law, as appropriate for government to do, and as requested by various industries.
  - Mandated by Homeland Security Act of 2002, but will likely not reach completion by end of 2006. Therefore Congress should commission a rapid-turnaround study to be conducted by the NAS with input from the private sector to compile a list of national priorities
  - Then these priorities should be used as a guide for allocation of resources and as a measure of effectiveness and progress toward bolstering national security.

- Strengthen DHS management and personnel experience, specifically by sponsoring and facilitating a personnel exchange with private sector.
  - DHS is currently plagued by high turnover, low morale, making it difficult to realize long-term initiatives – it needs experienced managers
  - Such an exchange program can be modeled after those employed at the Federal Reserve

- Improve information sharing with private sector, and government must be held accountable for doing it.
  - Private sector should be fully integrated, but there are reservations: businesses fear if they share information with the government it will be mishandled and could place them at a competitive disadvantage, and the government worries about leaking classified information to the private sector.

Appendix E – Glossary of Acronyms in this Report

AAF – Available Acquisition Flexibilities – form of acquisition flexibilities available in the Federal Acquisition Regulation (FAR) to facilitate and expedite acquisitions of supplies and services during all types of emergencies. "Available Acquisition Flexibilities" identifies the flexibilities that may be used anytime and do not require an emergency declaration.

ABA – American Bar Association – a voluntary bar association of lawyers and law students, which is not specific to any jurisdiction in the United States. The ABA's most important activities are the setting of academic standards for law schools and the formulation of model legal codes.

ARC – American Red Cross – a humanitarian organization that provides emergency assistance, disaster relief and education inside the United States, as part of the International Federation of Red Cross and Red Crescent Societies.

AWP – Average Wholesale Price

BENS – Business Executives for National Security – a national, non-partisan, non-profit organization that harnesses successful business models from the private sector to help strengthen the nation's security.

BOC – Business Operations Center

CFR – Council on Foreign Relations – an American foreign policy think tank based in New York City. It describes itself as being "dedicated to increasing America's understanding of the world and contributing ideas to U.S. foreign policy."

CI/KR – Critical Infrastructure/Key Resources – According to the Homeland Security Act of 2002, "critical infrastructure" refers to "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters." The term "key resources" means "publicly or privately controlled resources essential to the minimal operations of the economy and government."

DHS – Department of Homeland Security – a Cabinet department of the Federal Government of the United States with the responsibility of protecting the territory of the United States from terrorist attack and responding to natural disasters. The department was created from 22 existing federal agencies in response to the terrorist attacks of September 11, 2001.

EAF – Emergency Acquisition Flexibilities – a form of acquisition flexibilities available in the Federal Acquisition Regulation (FAR) to facilitate and expedite acquisitions of supplies and services during all types of emergencies. "Emergency Acquisition Flexibilities" identifies the flexibilities that may be used only after an emergency declaration or designation has been made by the appropriate official.

EMAC – Emergency Management Assistance Compact – an interstate agreement that streamlines the assistance one governor can lend another after a natural disaster or terrorist attack by providing a framework for flexible response. EMAC was first introduced to the states in 1993, and the program is administered by the National Emergency Managers Association (NEMA).

EOC – Emergency Operations Center – the central command and control facility responsible for carrying out emergency preparedness and emergency management or disaster management functions at a strategic level in an emergency situation, and for ensuring the continuity of operation of the company or political subdivision. The EOC is responsible for the strategic, or "big picture" of the disaster and does not normally directly control field assets but makes strategic decisions and leaves tactical decisions to lower commands.

ESF – Emergency Support Function – a mechanism that consolidates multiple agencies that perform similar or like functions into a single, cohesive unit to allow for the better management of emergency response functions.

FAR – Federal Acquisition Regulation – the Federal Acquisition Regulations System is established for the codification and publication of uniform policies and procedures for acquisition by all executive agencies. The Federal Acquisition Regulations System consists of the Federal Acquisition Regulation (FAR), which is the primary document, and agency acquisition regulations that implement or supplement the FAR.

FDIC – Federal Deposit Insurance Corporation – the FDIC preserves and promotes public confidence in the U.S. financial system by insuring deposits in banks and thrift institutions for at least $100,000; by identifying, monitoring and addressing risks to the deposit insurance funds; and by limiting the effect on the economy and the financial system when a bank or thrift institution fails.

FEMA – Federal Emergency Management Agency – an agency of the Department of Homeland Security (DHS) within the Emergency Preparedness and Response Directorate. FEMA's purpose is to coordinate the response to a disaster that has occurred in the United States and overwhelms the resources of local and municipal authorities.

FTC – Federal Trade Commission – an independent agency of the United States government, established in 1914 by the Federal Trade Commission Act. Its principal mission is the promotion of consumer protection and the elimination and prevention of anticompetitive business practices.

GAO – Government Accountability Office – the non-partisan audit, evaluation, and investigative arm of Congress, and an agency in the Legislative Branch of the United States Government. According to GAO's current mission statement, the agency exists to support the Congress in meeting its Constitutional responsibilities and to help improve the performance and ensure the accountability of the federal government for the American people.

GEOC – Georgia Emergency Operations Center – the central command and control facility responsible for carrying out the principles of emergency preparedness and emergency management or disaster management functions for the state of Georgia.

GSA – General Services Administration – an independent agency of the United States government, established in 1949 to help manage and support the basic functioning of federal agencies. The GSA supplies products and communications for U.S. government offices, provides transportation and office space to federal employees, and develops government-wide cost-minimizing policies, among other management tasks.

HHS – Health and Human Services – a Cabinet department of the United States government with the goal of protecting the health of all Americans and providing essential human services.

HIPAA – Health Insurance Portability and Accountability Act – law requiring HHS to establish national standards for electronic health care transactions and national identifiers for providers, health plans, and employers. It also addresses the security and privacy of health data.

ICS – Incident Command System – a management system used within the United States, parts of Canada, the United Kingdom and other countries to organize emergency response, designed to offer a scalable response to incidents of any magnitude. As part of FEMA's National Response Plan (NRP), the system has become part of the National Incident Management System (NIMS). The system is designed to grow and shrink along with the incident, allowing more resources to be smoothly added into the system when required or released when no longer needed.

INIPP – Interim National Infrastructure Protection Plan – the Base Plan that provides the framework and sets the direction for implementing a coordinated, national effort in the event of an incident. It provides a roadmap for identifying CI/KR assets, assessing vulnerabilities, prioritizing assets, and implementing protection measures in each infrastructure sector.

JFO – Joint Field Office – a temporary federal multiagency coordination center established locally to facilitate field-level domestic incident management activities related to prevention, preparedness, response, and recovery when activated by the Secretary.

MACS – Multiagency Coordination System – the combination of personnel, facilities, equipment, procedures, and communications integrated into a common system. When activated, the MACS has the responsibility for coordination of assisting agency resources and support in a multi-agency or multi-jurisdictional environment.

NEMA – National Emergency Management Association – a non-partisan, non-profit 501(c)(3) association dedicated to enhancing public safety by improving the nation's ability to prepare for, respond to and recover from all emergencies, disasters, and threats to America's security. The state directors of emergency management are the core membership of NEMA.

NERR – National Emergency Response Registry – permanent Internet-based system to source goods and services to the government in emergencies

NGO – Non-governmental organization – a non-profit group or association that acts outside of institutionalized political structures and pursues matters of interest to its members by lobbying, persuasion, or direct action.

NIMS – National Incident Management System – a system that integrates effective practices in emergency preparedness and response into a comprehensive national framework for incident management. The NIMS is meant to enable responders at all levels to work together more effectively to manage domestic incidents no matter what the cause, size or complexity.

NIPP – National Infrastructure Protection Plan – a document called for by Homeland Security Presidential Directive 7 which aims to unify Critical Infrastructure and Key Resource (CI/KR) protection efforts across the country.

NORTHCOM – U.S. Northern Command – a Unified Combatant Command of the United States Military created in 2002 in the aftermath of the September 11th attacks. Its mission is to protect the United States homeland and support local, state, and federal authorities, and it is responsible for U.S. military operations in the United States.

NPS – National Planning System

NRP – National Response Plan – a comprehensive all-hazards approach to enhance the ability of the United States to manage domestic incidents. The plan incorporates best practices and procedures from incident management disciplines—homeland security, emergency management, law enforcement, firefighting, public works, public health, responder and recovery worker health and safety, emergency medical services, and the private sector—and integrates them into a unified structure. It forms the basis of how the federal government coordinates with state, local, and tribal governments and the private sector during incidents.

OFPP – Office of Federal Procurement Policy – policy office within the Office of Management and Budget that plays a central role in shaping the policies and practices federal agencies use to acquire the goods and services they need to carry out their responsibilities. OFPP was established by Congress in 1974 to provide overall direction for government-wide procurement policies, regulations and procedures and to promote economy, efficiency, and effectiveness in acquisition processes.

QBL – Qualified Bidders List

SAIC – Science Applications International Corporation – Although SAIC is a large technology firm with numerous federal, state, and private sector clients, its traditional expertise has been supporting the United States Department of Defense and the Intelligence Community, including the National Security Agency.

SKU – Stock Keeping Unit – an identifier that is used by merchants to permit the systematic tracking of products and services offered to customers. SKUs are not always associated with actual physical items, but more appropriately billable entities.

SSA – Sector Specific Agency – Federal department or agency responsible for the overall coordination of planning, preparedness, and protection-related activities within each of the 17 CI/KR sectors.

TCL – Target Capabilities List – list of capabilities developed by the Department of Homeland Security that are required to prevent, protect against, respond to, and recover from incidents of national significance.

UTL – Universal Task List – a list of every unique task that was identified from the suite of Common Scenarios developed under the leadership of the Homeland Security Council. The fifteen scenarios address a range of probable threats from terrorists, natural disasters and other emergencies.

VOAD – Voluntary Organizations Assisting in Disaster – a coalition of various volunteer organizations with formal disaster response plans. These organizations share information about their capabilities, resources, and special areas of expertise in order to foster cooperation and reduce duplication of effort.

Appendix F – Public-Private Collaboration Outcomes and Drivers

State & Local Collaboration

Outcome:

- Build a "Business Operations Center" (BOC) capability in states and urban areas
  - Include critical infrastructure, disaster supply chain businesses and other critical businesses

Driver:

- Congress directs DHS to create guidelines and funding for states and urban areas to build BOCs
- Congress considers funding public-private communications systems and data links with direct appropriation; funding BOC sustaining costs through the federal grant program
- Congress directs DHS to tie receipt of funds to training and exercising

Achievability: High

Regional and Federal Collaboration

Outcome:

- Create an escalation process for public-private collaboration when increased federal participation is necessary

Driver:

- Congress directs DHS to create guidelines and funding for regional and federal BOCs (FEMA, JFO, other)

Achievability: High

Outcome:

- Integrate the BOC concept into the National Response Plan (NRP)

Driver:

- DHS to invite private-sector participation in developing and integrating the BOC concept into the NRP

Achievability: Moderate

"Business EMAC"

Outcome:

- Work with National Emergency Management Association (NEMA) to explore application of Emergency Management Assistance Compact (EMAC) model to private-sector resources

Driver:

- Task Force to nominate team to:
  - Validate "Business EMAC (BEMAC)" concept with NEMA
  - Seek support from the National Governors Association
- Congress provides funds through DHS to states for implementation

Achievability: High

Appendix G – Surge Capacity/Supply Chain Management Outcomes and Drivers

Emergency Purchasing

Outcome:
- Improve forecasting for emergency goods and services

Driver:
- FEMA improves forecasting model with other DHS offices and private-sector input and collaboration

Achievability: High

Outcome:
- Have pre-contracts in place and vendors pre-qualified

Driver:
- FEMA improves contracting and qualification mechanisms

Achievability: High

Outcome:
- Establish prices at the vendors' then-current market prices

Driver:
- FEMA and vendors establish pricing mechanisms

Achievability: Moderate

Outcome:
- Develop pricing mechanisms to be implemented in disaster situations

Driver:
- States take lead, working through affiliate associations to approach a national standard

Achievability: Moderate

Outcome:
- Establish mechanism for pre-qualifying before a crisis and for qualifying non-GSA or otherwise qualified vendors during a crisis

Driver:
- Governments create streamlined mechanisms for emergency certification

Achievability: High

Outcome:
- Establish more effective vendor selection mechanisms
  - Must have transparency of transactions
  - Be self-auditing

Driver:
- Governments develop mechanisms that include other vendor sources if pre-certified or otherwise qualified vendors cannot meet availability and delivery requirements.

Achievability: Moderate

Outcome:
- Further develop online "reverse auction" system for meeting ad hoc needs

Driver:
- Congress provides funding for NEMA to implement as part of "Business EMAC"

Achievability: Development of system: High; Funding: Moderate

Donations Management

Outcome:
- Identify most likely pro bono needs for a range of scenarios

Driver:
- FEMA improves forecasting model with business and NGO input and collaboration

Achievability: High

Outcome:
- Create online registry and reverse auction capability for meeting unanticipated needs for pro bono goods and services

Driver:
- Congress provides funding for NEMA to implement as part of "Business EMAC" within state EOC/BOC

Achievability: Development of process: High; Funding: Moderate

Logistics Processes

Outcome:
- Educate business employees and public on emergency preparations to lessen peak demand

Driver:
- Businesses provide employee education
- DHS continues improving website **www.ready.gov**

Achievability: High

Outcome:
- Improve credentialing process for private-sector responders and volunteers prior to and during disasters

Driver:
- States working with local authorities create standards and protocols
- Congress provides funding through DHS

Achievability: Moderate

Outcome:
- Improve "last mile" logistics to improve vehicle offloading and distribution capabilities

Driver:
- States and major urban areas working with local authorities develop capabilities

Achievability: Moderate

Appendix H – Legal & Regulatory Environment Outcomes and Drivers

Disaster Law: Liability

Outcome:

- Improve Good Samaritan protections with aim of ensuring predictability of liability

Driver:

- Congress and states develop common body of legislation or enact new law

Achievability: Low

Outcome:

- Clarify/standardize liability of professionals acting in good faith during disasters (e.g., patient triage, alternative treatments, etc.)

Driver:

- Congress improves legislation on the books or enacts new law

Achievability: Low

Disaster Law: Regulation

Outcome:

- Clarify and promulgate procedures that allow quick implementation of discretionary authorities during disasters
- Package and set triggers for implementation
  - Antitrust
  - Emergency implementation of environmental law
  - Licensing
  - Privacy
  - Service delivery and termination

Driver:

- Federal agencies review laws and authorities under their purview and make necessary changes

Achievability: High

Stafford Act

Outcome:

- Revise the Stafford Act to enable the private sector to:
  - Participate as full partners in the complete range of disaster response activities
  - Be afforded non-monetary federal assistance when necessary
  - Request assistance directly through the appropriate federal agency

Driver:

- Congress enacts revision

Achievability: Moderate

Congressional Hearings

Outcome:

- Identify recommendation from this report that can be implemented under existing authorities

Driver:

- Task Force uses its government affairs resources to encourage Congress to act

Achievability: High

Appendix I – Priorities and Sequencing

Business Integration into the National Response Plan

Outcome:

- Integrate business more fully in the federal, state and local government operations continuums:
  - Doctrine development
  - Capabilities-based resource planning
  - Operations planning
  - Training and exercises
  - Operations
  - Lessons-learned assessments

Driver:

- Congress directs DHS to include substantive business participation in federal programs
- Congress makes federal funds available to states for business participation

Achievability: Integration into NRP: High; Funding: Low

Resource commitment

Outcome:

- Ensure adequate resources are devoted to implementing Task Force recommendations at the state, regional and federal levels on a sustainable basis

Driver:

- Congress directs DHS to create guidelines and provide funding for states, urban areas, and regions to build sustainable partnerships to implement Task Force recommendations
- Task Force to consider a standing advisory group to:
  - Keep government and business focused in implementing the Task Force recommendations
  - Inform a core group of state governors and enlist their support for implementing the Task Force recommendations
  - Advise states, urban areas and regions on implementation of the recommendations
  - In cooperation with other like-minded groups (e.g., the Business Roundtable), develop a voluntary national-level advisory group that can offer advice and instruction to states interested in building a BOC structure

Achievability: Moderate

Business Executives for National Security

For a quarter century, Business Executives for National Security has been the primary channel through which American business leaders can contribute their special experience and talent to help build a more secure nation.

Founded in 1982 by business executive and entrepreneur Stanley A. Weiss, BENS is guided by the simple notion that America's security is everybody's business. Led by President and CEO General Charles G. Boyd, U.S. Air Force (Ret.), BENS is a national, nonpartisan organization of senior executives dedicated to enhancing our national security using the successful models of the private sector.

As the United States confronts threats of terrorism at home and abroad, BENS is more important than ever before. The innovative business-government partnerships that BENS has fostered over the past two decades to help save the Defense Department billions of dollars are now uniquely positioned to help meet the new challenges of the 21st century.

BENS is expanding these public-private partnerships into all aspects of homeland security – helping to guard against cyber attack, track terrorists' financial assets, secure the nation's ports, and prepare state and local governments to deal with catastrophic events or terrorist attacks.

Recognizing that the nation will never fully realize the efficient, agile military it needs to win a global war on terrorism without an equally efficient and agile support structure, BENS remains a tireless advocate for smarter spending at the Pentagon.

Responses to Questions from Marko Bourne

Question#:	1
Topic:	NIMS
Hearing:	Private Sector Preparedness, Part 1: Defining the Problems and Proposing Solutions
Primary:	The Honorable Daniel K. Akaka
Committee:	HOMELAND SECURITY (SENATE)

Question: The National Incident Management System (NIMS) Integration Center has recommended 12 practices for the private sector to support NIMS implementation. These activities parallel the implementation activities that have been required of State, territorial, tribal, and local governments since 2004.

Some funding is available to State and local governments to implement NIMS activities. Are there any incentives or technical assistance available to private business to encourage their participation?

If FEMA collects data on private sector adoption of these recommendations, please describe the results. If FEMA does not collect such data, please explain why it does not and how it monitors private sector support of NIMS implementation.

Answer: On November 30, 2006, FEMA posted a fact sheet of recommended activities for the private sector, which parallel activities recommended for State and local government entities. These activities include: 1) adopting the NIMS; 2) identifying emergency points of contact and sharing the information with the local emergency management authority; and 3) adopting the use of the Incident Command System (ICS). This fact sheet can be found at: http://www.fema.gov/pdf/emergency/nims/ps_fs.pdf.

In response to the funding question, some funding is available to infrastructure sectors in the form of grants from the Department of Homeland Security's Infrastructure Protection Program (IPP). For fiscal year (FY) 2007, the IPP is comprised of five separate grant programs: the Transit Security Grant Program (TSGP), the Port Security Grant Program (PSGP), the Intercity Bus Security Grant Program (IBSGP), the Trucking Security Program (TSP), and the Buffer Zone Protection Program (BZPP). FY 07 funding under these grant programs totaled roughly $445 million for State, local and private industry infrastructure protection initiatives. Together, these grants fund a range of preparedness activities, including strengthening infrastructure against explosive attacks, planning, equipment purchase, training, exercises, and security management and administration costs. IPP programs support objectives outlined in the interim National Preparedness Goal, the National Response Plan, NIMS, and the National Infrastructure Protection Plan. While there are no specific incentives to encourage NIMS implementation in the private sector, the IPP grant programs require that recipients of these funds implement the NIMS. Official monitoring of NIMS adoption, as required by these programs, occurs during the grant monitoring process.

In terms of monitoring NIMS adoption by the private sector, while FEMA does collect data on State and local government adoption of NIMS, we do not specifically collect data on private sector compliance. However, the data collection tool that FEMA uses is being expanded to include hospital and health care compliance and will eventually include other private sector partners. The data collection tool allows FEMA to identify gaps in NIMS compliance and offer technical assistance to the users.

Question#:	2
Topic:	loaned business executive program
Hearing:	Private Sector Preparedness, Part 1: Defining the Problems and Proposing Solutions
Primary:	The Honorable Daniel K. Akaka
Committee:	HOMELAND SECURITY (SENATE)

Question: Your written testimony mentions FEMA's Loaned Business Executive Program to bring experts from the private sector into FEMA to serve as advisors and collaborate on mission critical programs. This initiative could facilitate the exchange of knowledge and expertise between the private sector and FEMA.

Please describe how the program will operate; when it is scheduled to begin; the expected number of participants and length of assignments; and the anticipated qualifications and background of participants.

Answer:

In an effort to raise the level of understanding and knowledge of each other's resources, capabilities, and levels of sufficiency that can be leveraged to prevent, protect against, respond to, recover from all hazards, FEMA seeks improved collaboration with private sector entities. To this end, FEMA is piloting a program in which expert employees of private sector entities will be systematically integrated into FEMA through a loaned executive program, on a temporary basis, that not only will allow private sector executives to lend their insights and best practices to FEMA's operations, but will also serve to improve their own understanding of Federal policies, processes, priorities and actions related to emergency management and preparedness.

As the primary owner of industry infrastructure and/or the manufacturer of the majority of consumable and durable goods used by Federal, State and local entities to respond to a disaster, it is vital that the private sector be engaged by the Federal government in a productive and collaborative manner to help ensure the nation is prepared to respond to and recover from all hazards. The following program structure is designed with this objective in mind.

AUTHORITY AND IMPLEMENTATION

This program is established pursuant to 5 U.S.C. 3109, 5 C.F.R. Part 304; and Section 832 of the Homeland Security Act (codified at 6 USC 392), which authorizes appointment of "experts or consultants" in accordance with 5 USC 3109, and Department of Homeland Security Management Directive (MD) 3010.2, "Employment of Experts and

Question#:	2
Topic:	loaned business executive program
Hearing:	Private Sector Preparedness, Part 1: Defining the Problems and Proposing Solutions
Primary:	The Honorable Daniel K. Akaka
Committee:	HOMELAND SECURITY (SENATE)

Consultants," dated March 22, 2004. FEMA implements and administers this Program in accordance with Agency policy as provided by the Office of Management.

PROGRAM DESCRIPTION

The FEMA Private Sector Loaned Executive Program provides a formal process to engage employees of private sector organizations in FEMA work. This program will provide FEMA with a better understanding of private sector resources and capabilities. Likewise, upon expiration of the Federal appointment, the private sector employee will have a better understanding of government resources and capabilities as they relate to emergency management and preparedness in an all hazards environment.

Appointees will be assigned to one of the main line directorates within FEMA, beginning with Logistics, Disaster Operations, and Disaster Assistance. This will expose appointees to a wide ranging spectrum of emergency management and preparedness operations and activities. They will be involved in providing insight, both technical and analytical in nature, in the development, revision, and refinement of a wide range of new and existing processes, policies and procedures, and systems. In order to avoid conflict of interest, during the time of their tenure at FEMA, appointees will be barred from working on matters (i.e. contracts) that are before their private sector organizations.

Selections

The Administrator of FEMA shall approve final selection for appointment. Approved selections must meet the strategic program goals of FEMA. The expected public benefit realized through improved FEMA and private sector mutual understanding and the experience of the candidate will be primary considerations in making selections.

Appointments

After coordination and approval of a formal written agreement, offers of appointment will be made by FEMA and administered by HR in accordance with applicable policies, laws, rules, and regulations. FEMA HR will make appropriate arrangements per existing policies and procedures for the individual's entry on duty to include the report date, new employee orientation, security badging, etc. Although unpaid, appointments will be to positions at the grade and step level equivalent to GS-15 step 10 and below.

FEMA **may not** use 5 USC 3109 as a basis for authority to appoint individuals:

Question#:	2
Topic:	loaned business executive program
Hearing:	Private Sector Preparedness, Part 1: Defining the Problems and Proposing Solutions
Primary:	The Honorable Daniel K. Akaka
Committee:	HOMELAND SECURITY (SENATE)

- To a position requiring Presidential appointment. However, subject to the conditions of this part, an agency may appoint an individual awaiting final action on a Presidential appointment to an expert or consultant position.

- To a Senior Executive Service (SES) position.

- To perform managerial or supervisory work (although an expert may act as team leader or director of the specific project for which he/she is hired), to make final decisions on substantive policies, or to otherwise function in the agency chain of command (e.g., to approve financial transactions, personnel actions, etc.).

- To do work performed by the agency's regular employees (with the exception of project work related to program goals and objectives where the executive may work on a team with regular FEMA employees).

- To fill in during staff shortages.

- Solely in anticipation of giving that individual a career appointment. However, subject to the conditions of this part, an agency may appoint an individual to an expert or consultant position pending Schedule C appointment or non-career appointment in the Senior Executive Service.

Candidate's Qualifications

For both the private sector and FEMA to realize the maximum benefit from this program, private sector personnel must have a certain level of operational or technical experience. *Ideal candidates for participation in the process would be current division or line managers with broad operational and technical experience.* A more comprehensive listing of qualifications is provided in the "Private Sector Loaned Executive Candidate Position Description and Qualifications" below but, in short, candidates would have about 10 years experience in performing or supporting their duties. A security clearance will not be required.

Eligibility for Appointment

To be eligible for an appointment to FEMA under this program, in addition to meeting the requirements of 5 C.F.R. Part 304, candidates must meet citizenship requirements for

Question#:	2
Topic:	loaned business executive program
Hearing:	Private Sector Preparedness, Part 1: Defining the Problems and Proposing Solutions
Primary:	The Honorable Daniel K. Akaka
Committee:	HOMELAND SECURITY (SENATE)

Federal employment in accordance with 5 C.F.R. 302.203, as well as any other regulatory or statutory limitation.

Length of Appointment

There are several approaches available to management regarding the length of appointment and any extensions to the initial appointment. These approaches are provided under 5 C.F.R. 304.103(c) which is summarized as follows:

(a) Approach I: Initial appointments for full time positions may be made for a period not to exceed one year. The expert or consultant may be reappointed for one additional period not to exceed one year.

(b) Approach II: Initial appointment for a part time or seasonal position, not to exceed six month service during the appointment period. The expert or consultant may be reappointed under the same limitations in one year increments without limitation.

- Example: Experts or consultants initially appointed to a one year part time appointment with a work schedule of one week per pay period. Appointment renewed without limitation.

(c) Approach III: Initial appointment for an intermittent position, not to exceed six month service during the appointment period. The expert or consultant may be reappointed under the same terms in one year increments without limitation.

- Example: Expert or consultant initially appointed to a one year intermittent appointment with no pre-set work schedule. Management calls expert or consultant to work as needed, but must track service so as not to exceed the six month limitation. The expert or consultant may be reappointed under the same terms in one year increments without limitation.

(d) 5 C.F.R. 304.103(c) provides that in the event the expert or consultant exceeds six months service during an initial appointment, they may be reappointed for one additional year. An expert or consultant who exceeds the six month limitation in any subsequent year may not be reappointed thereafter.

Termination of Appointment

Question#:	2
Topic:	loaned business executive program
Hearing:	Private Sector Preparedness, Part 1: Defining the Problems and Proposing Solutions
Primary:	The Honorable Daniel K. Akaka
Committee:	HOMELAND SECURITY (SENATE)

Appointments may be terminated by FEMA at any time it is determined that the services of the expert or consultant are no longer needed or when the expert or consultant is not performing at an acceptable level.

(a) Specific procedures will be discussed with FEMA HR in advance of notifying any expert or consultant of termination.

(b) Experts and consultants appointed under 5 USC 3109 are considered "excepted service" employees and will have appeal rights only after 2 years of current continuous service in the same or similar position in an Executive Agency.

Written Agreements

As a condition of employment, the appointee will sign a written agreement outlining the roles, expectations, and limitations of the position to which they are appointed. The written agreement must include, but is not limited to, the following elements:

- The duties to be performed, duration, and terms under which extensions to the appointment may be granted.
- The obligations and responsibilities of the expert or consultant and FEMA.
- The ethics and security restrictions regarding outside employment with their private sector organization while a federal employee.
- Any post employment ethical restrictions.

The agreements will be approved in advance of hiring for each FEMA expert or consultant by FEMA HR, OCC Ethics Counsel and OCC – General Law. Agreement templates are provided as appendices to this document.

Information for Private Sector Employers

FEMA can provide information for prospective experts and consultants to share with their private sector employers explaining the program. However, it is the responsibility of the expert or consultant to approach their private sector employer to request release from their regular duties to accept the Federal appointment. Recruitment information describing the program may be provided to private sector employers or otherwise distributed to generate potential candidates for this program. At a minimum, such information will be coordinated with FEMA HR, OGC Ethics Counsel, OGC – General Law, and External Affairs prior to release.

Question#:	2
Topic:	loaned business executive program
Hearing:	Private Sector Preparedness, Part 1: Defining the Problems and Proposing Solutions
Primary:	The Honorable Daniel K. Akaka
Committee:	HOMELAND SECURITY (SENATE)

Duty Location

The duty station is established in Washington, D.C. for these positions do to the following reasons:

(a) Generally, an individual is appointed to the duty location where they are expected to perform work for the agency. If the work is to be performed in Washington, D.C., the duty location must be Washington, D.C.

(b) Although FEMA is authorized to pay relocation expenses for new appointees under 5 C.F.R. Part 572, paid relocation for new Federal appointments is rarely used.

(c) There would be no authority to pay travel expenses for the expert or consultant to return to his private sector employer's facilities.

Reporting Requirements

5 C.F.R. 304.107 does not establish a reporting requirement regarding the use of ***unpaid*** experts or consultants appointed under 5 C.F.R. Part 304. However, the following internal reporting is required:

(a) Consistent with the provisions of MD 3010.2, "Employment of Experts and Consultants," at the request of FEMA HR, each FEMA directorate where an expert or consultant is employed shall provide a listing of current expert and consultant appointments.

- This report will provide the nature of the appointment, the name of the individual, a statement that the expert or consultant is unpaid, a brief statement of the purpose, and the duration of the appointment.

(b) Any request for an extension of an appointment, or a reappointment after a break in service, shall include a detailed description of previous appointments including the information contained in (a) plus the number of days or hours the expert or consultant worked in the previous appointment.

Terms and Conditions

An individual appointed under 5 C.F.R. Part 304 **is a Federal employee** for most purposes and is subject to applicable rules and regulations regarding Federal employment. This includes, but is not limited to: 18 U.S.C. Chapter 11 (Bribery, Graft,

Question#:	2
Topic:	loaned business executive program
Hearing:	Private Sector Preparedness, Part 1: Defining the Problems and Proposing Solutions
Primary:	The Honorable Daniel K. Akaka
Committee:	HOMELAND SECURITY (SENATE)

and Conflicts of Interest); 18 U.S.C. 1905 (Disclosure of Confidential Information Generally); 28 U.S.C. 1346 (b), and 28 U.S.C. 2671 et seq. (Federal Tort Claims Act); 5 U.S.C. Chapter 81 (Compensation for Work Injuries); 5 C.F.R. Part 2635 (Standards of Ethical Conduct for Employees of the Executive Branch).

Private Sector Loaned Executive Candidate Position Description and Qualifications

1. Logistics

Objective: To establish a private sector "loaned executive" program in the FEMA Logistics Directorate to assist in sharing knowledge of commercial supply chain capabilities and to explore potential areas for appropriate private sector engagement in disaster logistics.

Goals:

- Provide private sector with insight into Federal agency management and current approach to disaster preparedness emergency management.
- Assist FEMA Disaster Logistics to better understand the private sector logistics processes and capabilities and how they may be employed to provide logistics assistance.
- Demonstrate the value of commercial and government collaboration and partnership.
- Identify commercial best practices and initiate steps to import them into FEMA logistics operations, to include but not be limited to sourcing, distribution, warehousing and transportation, accounting and asset tracking/visibility.

Concept and timeline based on a 6-to-9-month program (all dates are tentative):

- Program Kick-off and FEMA Welcome & Orientation. Provide an overview of the New FEMA, its Mission and Vision, core competencies, organizational structure, and roles and responsibilities.
- Disaster Logistics orientation – visit to a Distribution Center; overview of Distribution and Logistics Centers and PEPs; brief on current FEMA National logistics footprint, assets, and capabilities; brief on current systems and Total Asset Visibility program objectives.
- Report directly to Mark Snyder, Senior Logistics staff, on a day-to-day basis for new tasking and on-going projects; participate in all senior level meetings.
    - On-going projects; logistics planning for hurricane season.
    - Planning strategy for adopting a 3rd party logistics provider structure.
    - Inventory management strategy with private sector.

Question#:	2
Topic:	loaned business executive program
Hearing:	Private Sector Preparedness, Part 1: Defining the Problems and Proposing Solutions
Primary:	The Honorable Daniel K. Akaka
Committee:	HOMELAND SECURITY (SENATE)

  - Addressing short-term and longer-term recommendations resulting from 90-day logistics assessment by SiloSmashers, a management and technology consulting company contracted by FEMA.
- Potential for temporary relocation to the field in the event of JFO stand-up for a hurricane or other disaster; on-going projects; logistics planning; systems modernization.

Potential Projects and Responsibilities:

- Provide report on planning, preparedness and response capability of various private sector entities in disaster management with particular emphasis on potential applicability and transference of commercial processes and technology to FEMA
- Provide a Strengths, Weaknesses, Opportunities and Threats (SWOT) analysis on specific commercial supply chain processes (e.g., inventory management, transportation, systems visibility, technical assets) particularly as related to potential support of FEMA Disaster Logistics
- Provide report on beneficial commercial contracting practices that could be used in government contracting of disaster supplies and services (includes discussion of strategy for adoption of a third party logistics provider structure)
- Provide a report on commercial technologies that could be adopted by the government for sourcing, distribution, warehousing and transportation, accounting and asset tracking/visibility
- Individual training and professional development best practices

Qualifications: Individual should have these general private sector qualifications

- 10 years commercial business experience
- Expertise in (or access to) contracting management
- Expertise in (or access to) IT management
- Expertise in logistics and supply chain management

2. Disaster Operations

Objective: To establish a private sector fellowship program in new FEMA Disaster Operations directorate to assist in building knowledge of commercial capabilities and to explore potential areas for appropriate private sector engagement in disaster response and operations.

Goals:

Question#:	2
Topic:	loaned business executive program
Hearing:	Private Sector Preparedness, Part 1: Defining the Problems and Proposing Solutions
Primary:	The Honorable Daniel K. Akaka
Committee:	HOMELAND SECURITY (SENATE)

- Assist FEMA to better understand private sector processes, capabilities and capacities and how they could be employed to support the Federal response to a disaster. Potential areas of interest include but are not limited to:
    - Conduct of disaster operations
    - Information sharing and information transfer
    - Maintaining situational awareness
    - Commercial contact and coordination
    - Operational planning
- Identify commercial best practices and initiate steps to import them into FEMA Disaster Operations.
- Identify commercial technology that could improve disaster operations and response.
- Review Katrina Lessons Learned and identify potential areas where private sector resources and/or capabilities could be leveraged to enhance response capabilities for 2007 hurricane season and beyond.

Concept and timeline based on a 9-month program (all dates are tentative):

- Program Kick-off and FEMA Welcome & Orientation. Provide an overview of New FEMA, its Mission and Vision, core competencies, organizational structure, and roles and responsibilities.
- Disaster Operations orientation
- Report directly to Disaster Operations senior leadership on a day-to-day basis for new tasking and on-going projects; participate in all senior level meetings.
- On going projects; planning for hurricane season
- Potential for temporary relocation to the field in the event of JFO stand-up for a hurricane or other disaster; on-going projects

Potential Projects and Responsibilities:

- Provide report on planning, preparations and response capability of various private sector entities in disaster management with particular emphasis on potential applicability and transference of commercial processes and technology to FEMA.
- Provide insight into operations and strategic planning practices that could be used in FEMAs Disaster Operations directorate and pushed into the field at the Regional and Joint Field Office level.
- Provide a report on commercial technologies that could be used to improve disaster response capabilities.
- Help develop a concept paper and execution plan for building a private sector liaison capability in the JFO structure.

Question#:	2
Topic:	loaned business executive program
Hearing:	Private Sector Preparedness, Part 1: Defining the Problems and Proposing Solutions
Primary:	The Honorable Daniel K. Akaka
Committee:	HOMELAND SECURITY (SENATE)

Qualifications: Individual should have these general private sector qualifications:

- 10 years commercial business experience
- Expertise in operations management
- Expertise in strategic planning
- Expertise in crisis management

3. Disaster Assistance

Objective: To establish a private sector fellowship program in FEMA's Disaster Assistance Directorate to assist in sharing knowledge of commercial capabilities and to explore potential areas for appropriate private sector engagement in disaster assistance.

Goals:

- Assist FEMA to better understand what an appropriate role for the private sector should be in the identification, planning, and coordination of volunteers and donated resources.
- Assist FEMA in developing procedures for accepting resources and donations from the private sector.
- Assist FEMA in the development of procedures to enable FEMA to purchase product from the private sector in a very timely manner (e.g. manufactured housing).
- Provide private sector with insight into Federal agency management and approach to disaster assistance and emergency management.
- Demonstrate the value of commercial and government collaboration and partnership.

Concept and timeline based on a 9-month program (all dates are tentative):

- Program Kick-off and FEMA Welcome & Orientation. Provide an overview of the New FEMA, its Mission and Vision, core competencies, organizational structure, and roles and responsibilities.
- Disaster Assistance directorate orientation.
- Report to both a Disaster Assistance directorate leadership POC and to the Leader for VOLAG/Donations Unit, ESF #6 Section for on-going project involvement opportunities and new tasking; participate in senior level meetings and briefings as appropriate.
- On-going projects, such as planning for hurricane season.
- Potential for temporary relocation to the field in the event of JFO stand-up for a hurricane or other disaster; on-going projects.

Question#:	2
Topic:	loaned business executive program
Hearing:	Private Sector Preparedness, Part 1: Defining the Problems and Proposing Solutions
Primary:	The Honorable Daniel K. Akaka
Committee:	HOMELAND SECURITY (SENATE)

Potential Projects and Responsibilities:

- Provide guidance in the development of established procedures for the intake, processing, and use of donated resources from the private sector to include a communications strategy.
- Provide guidance in the development of established procedures for expedited purchase and receipt of product from the private sector (e.g. manufactured housing)
    - May include Indefinite Delivery/Indefinite Quantity (IDIQ)contracts
- Provide technical assistance on matters relating to domestic and international corporate donations management (international corporate donations can present unique challenges).
- Participate in the study and analysis of recovery operations and assist in the identification of appropriate coordination mechanisms with the private sector.
- Provide input into the efficient, effective, and timely management of information related to volunteer and donations management, including making recommendations on specific information to be made available to the private sector and identifying specific outreach mechanisms.
- Support the ongoing development of a donations management database and the development and delivery of related stakeholder training and professional development.

Qualifications: Individual should have these general private sector qualifications

- 10 years commercial business experience
- Strong written and oral communication skills
- Expertise in project management, including monitoring and evaluating project performance, staff and resources
- Expertise in using computer technology to develop and maintain project related materials, including briefing papers, presentations, budgets, and databases
- Demonstrated organizational skills and ability to prioritize, plan, and execute tasks under tight deadlines

Current Status

FEMA has reached agreement with UPS to send us one of their executives in logistics for a period of time between 6-8 months to assist the Logistics Directorate. The timeline for selection of this individual and getting him onboard at FEMA is expected to take place during the month of August.

FEMA views this first loaned executive as a "pilot" from which to take lessons learned that can be applied to improve our program as we decide whether to bring on executives from other companies in the future in other areas of the organization.

Question#:	3
Topic:	private sector registry
Hearing:	Private Sector Preparedness, Part 1: Defining the Problems and Proposing Solutions
Primary:	The Honorable Mary L. Landrieu
Committee:	HOMELAND SECURITY (SENATE)

Question: During hurricanes Katrina and Rita, FEMA did not have the capability to match needs on the ground with available resources from the private and nonprofit sectors. What is the status of the contractor, AIDMATRIX's, efforts to create a National Emergency Resource Registry that can provide this capability in real-time?

Answer:

FEMA provided a grant in FY06 to the Aidmatrix Foundation, a non-profit with experience in creating donations management software, to develop a web-based application for the general public, including the private sector, to register their offers of donated goods in disasters. The donations management component of this information-management resource tool is complete and ready for use by States and their State Donations Coordination Teams to view offers of donated goods in real-time. FEMA is in the process of signing up States in order to provide the access to this free tool, and to provide the necessary training required.

Question#:	4
Topic:	FEMA reimbursements
Hearing:	Private Sector Preparedness, Part 1: Defining the Problems and Proposing Solutions
Primary:	The Honorable Mary L. Landrieu
Committee:	HOMELAND SECURITY (SENATE)

Question: FEMA's Public Assistance system requires local governments to await reimbursement for their expenses, which can take several months. Private companies who are contracted at the local level to perform emergency work must endure this same waiting period before they can pay their employees or cover their own expenses. Many small and local businesses could not afford to wait during the response to Katrina and Rita, and felt betrayed that they rushed in to help, and were forced to wait months for reimbursement by the federal government. How is FEMA correcting the reimbursement lag time, and its negative impact on businesses who respond to disaster needs?

Answer:

The Public Assistance Program staff works with State and local governments to develop scopes of work in order to estimate the eligible costs for response activities, debris removal operations, and permanent restorative work. The eligible costs are captured on and financed (obligated) through Project Worksheets (PW). Based on its value, a PW is classified as either a small project or a large project. For FY07, projects estimated less than $59,700 are classified as small projects. The importance in the classification determines how the State (Grantee) can disburse Public Assistance grant funds. The Grantee can disburse the federal share of small projects to the local governments as soon as the project is obligated. The Grantee pays large projects on a reimbursement bases. As a local government incurs cost, it submits invoices to the Grantee and the Grantee reimburses based on eligible cost spent.

FEMA's Public Assistance Program is offering to State and local governments the opportunity to participate in a pilot procedure that allows accepting a grant based on an estimate for projects less than $500,000. This pilot procedure allows disbursement of the federal share of the project as soon as the project is approved. This pilot procedure differs from our current large project process where the payment is typically made after work is completed on a reimbursement bases.

The pilot procedure allows the local government to have the funds readily available. This pilot procedure is open to all Public Assistance disasters during the period of June 1, 2007 until December 31, 2008. This pilot procedure is not available for reimbursement for damages caused by Hurricanes Katrina and Rita.

Question#:	5
Topic:	Hurricane Preparedness Exercise
Hearing:	Private Sector Preparedness, Part 1: Defining the Problems and Proposing Solutions
Primary:	The Honorable Mary L. Landrieu
Committee:	HOMELAND SECURITY (SENATE)

Question: In your testimony, you mention the private sector's involvement in the National Exercise Division's annual Hurricane Preparedness Exercise. Can you please elaborate on recent hurricane exercises held, actors involved, and lessons learned?

Answer:

In 2006, the Department of Homeland Security (DHS) sponsored regional hurricane preparedness tabletop exercises to increase the preparedness of the Nation for the 2006 hurricane season. Building upon the successes of the 2006 effort, the Department conducted a national level functional exercise as well as a number of regional hurricane preparedness workshops in preparation for the 2007 hurricane season.

The national level functional exercise (Ardent Sentry-Northern Edge 07 (AS-NE 07)) took place in FEMA Region I (May 8-11, 2007). Regional workshops were conducted in Regions IV, VI, and IX. The regional workshops provided an opportunity to review and validate the regional Hurricane Concept of Operations (CONOPS) and an opportunity to synchronize the regional CONOPS with State and national plans prior to the 2007 hurricane season. The discussion based exercises were conducted as a "workshop" as identified in the Homeland Security Exercise and Evaluation Program (HSEEP). The workshop focused on the following discussion points: Management; Emergency Services; Mass Care, Housing and Human Services; Communications; Infrastructure; and Logistics.

Approximately 100 members of the Region IV Regional Interagency Steering Committee (RISC) participated in their regional workshop on May 3, 2007. There were approximately 125 participants as part of the Region VI workshop conducted on March 29, 2007. Approximately 170 participants, including the Region IX RISC, participated in the Region IX workshop conducted on May 22 and 23, 2007. Participants in all three workshops included federal representatives from Emergency Support Function (ESF) organizations, FEMA Regional headquarters representatives, nongovernmental organizations, State and regional agencies and stakeholders.

The after-action reports examine the issues identified during the workshops and provide comments in two distinct areas. First, the report outlines stakeholder concerns as they relate to national level issues. Second, the report provides an issues/actions matrix specifically designed for participants from the specific region.

The regional after-action reports for Region IV, VI and IX did not focus specifically on the private sector. However, Region IV identified the necessity to coordinate with private sector businesses to ensure inclusion in disaster response planning. Region IX identified the importance of drafting the CONOPS to be addressed to local and private sector audiences. Further, the regions stressed the importance of including the private sector in joint planning when discussing mass care, housing and infrastructure.

Post-Hearing Questions for the Record

Submitted to Duane Ackerman, Former BellSouth CEO;

Chairman of the BENS Business Response Task Force.

From Senator Daniel Akaka

1. In 2000, BellSouth, then under your leadership, and FEMA co-hosted the LIFELINE: Project Impact Business Summit, which sought to use the Project Impact program to encourage business and government leaders to collaborate on disaster planning and recovery.

   What is your view on the value of the Project Impact program? Do you believe that Congress should restore funding for programs like Project Impact?

   Answer: The Private Sector owns and operates the vast majority of the capability required to provide adequate disaster response and recovery. In fact, it is the PRIVATE Sector, through contracts with FEMA, state Emergency Management Agencies and other government entities which provide those capabilities today. The issue being addressed by the Business Response Task Force (BTRF) is how to create a more effective and efficient disaster response mechanism by systematically integrating the capabilities of business into the emergency response process at all levels. To do so requires trusted and dynamic environments where government can engage the private sector in information sharing, issue analysis and problem solving. In a sense, the role of government changes from a broker responsible for the procuring of resources and capabilities to a coordinator/facilitator responsible for guiding

the procurement process. In this model, the private sector becomes an active participant in all aspects of disaster response from pre-event planning through response activities into the recovery process.

The BTRF recommendations provide for the formalization of the required Public/Private Partnership in a structural way by the formation of Business Operations Centers which will operate as integral components of governmental response structures and provide a means of constant business involvement not just ad hoc involvement during a disaster. The funding necessary to establish and sustain these partnerships should be embedded within the recurring grant process for Federal, state and local emergency management capability rather than through stand alone programs or one time projects.

2. The Business Executives for National Security (BENS) Task Force is undertaking critical work to integrate systematically the capabilities of the business community into a comprehensive national response mechanism.

   In the aftermath of a disaster, vulnerable groups-- including the poor and patients in hospitals or nursing homes often have the most serious and pressing needs.

   How does the BENS Task Force work ensure that the needs of vulnerable populations are identified, understood and incorporated into disaster preparations and response plans?

   Answer: The members of the Business Response Task Force (BTRF) fully recognize that any effective response to a disaster must be comprehensive; not only in scope as it relates to the

resources and capabilities required but also in reach as it relates to the population affected by the disaster. To emphasize this point, the Task Force Report puts forth the notion of Continuity of Community. Continuity of Community recognizes that the community is a whole made up of many and various members and that if all members are not served by disaster response, the community as a whole is underserved. Preparation for disaster response must be built through a thorough understanding of the Community; who are its members; what outcomes constitute the socio-economics well being of the Community; who provides for those outcomes; what resources and capabilities are necessary for the desired outcomes to be realized, etc.

The most effective disaster response restores the Community to a self-sustaining level as quickly as possible following a disaster event. In this way, government is relieved from responsibility for the response effort sooner; commercial activities return to normal and social needs are met through normal means. To achieve this result, the private sector entities who are vital to the normal functioning of the community must fully participate in the comprehensive disaster response effort.

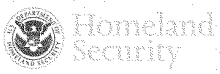
From Senator Mary Landrieu

1. In your testimony, you mention the need for some companies to be given emergency responder status, and the need for access and credentialing of their employees. I have proposed legislation, known as the First Response Broadcasters Act that would address these needs for the broadcaster community. I would like to ask whether you are familiar with the bill, and if so, as someone with a

background in telecommunications and knowledge of emergency management, I would like to hear your opinion of the proposal.

Answer: The First Response Broadcasters Act of 2007 touches on many of the issues necessary for critical infrastructure providers and operators to be effective in their restoration efforts following a disaster. Specifically, the Act highlights the following issues as critical to the Broadcast industry; access to the disaster area; credentialing of employees, contractors and agents; priority access to fuel, water and other resources necessary to carry out restoration efforts; and the potential need for protection of employees and property during periods of civil unrest. These issues must also be addressed for critical infrastructure owners and operators. Solutions for these issues could be accommodated for all appropriate groups through amendments to the Stafford Act with emergency responder status being afforded to a group of named industries and organizations. The Broadcast industry could be included in this list if they are deemed critical for a comprehensive disaster response effort. Issues associated with adequate investment in broadcast technology and infrastructure are best left to the various regulatory agencies with industry oversight responsibility rather than being included in disaster response legislation.

Sector-Specific Agency	Critical Infrastructure/Key Resources Sector
Department of Agriculture Department of Health and Human Services	Agriculture and Food
Department of Defense	Defense Industrial Base
Department of Energy	Energy
Department of Health and Human Services	Public Health and Healthcare
Department of the Interior	National Monuments and Icons
Department of the Treasury	Banking and Finance
Environmental Protection Agency	Drinking Water and Water Treatment Systems
Department of Homeland Security	
Office of Infrastructure Protection	Chemical Commercial Facilities Dams Emergency Services Nuclear Reactors, Materials, and Waste
Office of Cyber Security and Telecommunications	Information Technology Communications
Transportation Security Administration	Postal and Shipping
Transportation Security Administration, United States Coast Guard	Transportation Systems
Immigration and Customs Enforcement, Federal Protective Service	Government Facilities



For questions or more information, please contact NIPP@dhs.gov or visit www.dhs.gov/nipp.