

GEORGE MASON UNIVERSITY SCHOOL OF LAW
CRITICAL INFRASTRUCTURE PROTECTION (CIP)
PROGRAM

WEDNESDAY, SEPTEMBER 27, 2006
11:00-2:00 p.m.

WELCOME AND INTRODUCTION:
JOHN MCCARTHY,
DIRECTOR AND PRINCIPAL INVESTIGATOR, CIP PROGRAM

SPEAKER:
GEORGE FORESMAN,
UNDER SECRETARY FOR PREPAREDNESS,
DEPARTMENT OF HOMELAND SECURITY

MODERATOR AND INTRODUCTIONS:
JEANNE MESERVE,
WASHINGTON-BASED CORRESPONDENT, CNN

PANEL:

DAVID EISNER, CHIEF EXECUTIVE OFFICER,
CORPORATION FOR NATIONAL COMMUNITY SERVICE

PAUL KURTZ, EXECUTIVE DIRECTOR,
CYBER SECURITY INDUSTRY ALLIANCE

DON NOZNESKY, DIRECTOR OF CORPORATE SECURITY,
FPL GROUP INC.

HARRY OELLRICH,
MANAGING DIRECTOR AND HEAD OF CYBER TECHNOLOGY AND
INTELLECTUAL PROPERTY PRACTICE,
GUY CARPENTER INSURANCE

JOHANNA SCHNEIDER,
EXECUTIVE DIRECTOR - EXTERNAL RELATIONS,
BUSINESS ROUNDTABLE

THE NATIONAL PRESS CLUB
WASHINGTON, D.C.

JOHN MCCARTHY: Good afternoon, everyone. Good afternoon. I hate to break up good conversation, but we'd like to get our program launched here. I'm John McCarthy of the Critical Infrastructure Protection Program at George Mason University Law School. Welcome to our next in a series of *Critical Conversations* that we have sponsored for three years here at the Press Club. Our goal with the *Critical Conversation* is to bring together the public and private sector dialogue and to bring together thought leaders and ask them hard questions. That's our goal today.

The CIP Program began nearly four years ago with a goal of building a research curriculum and an outreach curriculum that was broader than just one university. We partnered with James Madison University and have worked with dozens, literally dozens, of other universities and professors around the entire nation, and internationally, I should say. The goal is to bring together the disciplines of law, policy, technology, economics, and to bring them to bear in a coordinated way on these complex and difficult problems that the nation faces relative to our infrastructures.

We have been very fortunate to have an exceptional executive agent in the Department of Commerce's National Institute of Standards of Technology. They have given us a broad charter to be able to explore – hopefully, people would say – in an innovative way this diverse curriculum. NIST has not limited it based on bureaucracy and we appreciate that very much.

I would like to note before I introduce some folks the passing of a person I consider a great American, Admiral J. William Kime, the 19th commandant of the Coast Guard. He'll be buried in Arlington on Friday. And other than having served as his aide and him being a personal mentor to me, he is very, very important to this curriculum, this discipline, this dialogue.

Admiral Kime I think will be most noted for two things that are important to critical infrastructure. First, he oversaw one of the largest restructurings in government after the Exxon Valdez incident. And he was one of the first individuals who thought through the notion of an incident of national significance and how the government and the private sector needed to interface under those circumstances. So one-and-a-half decades ago, he sat down and began to think through the very issues that people like our guest speaker today face every day.

The other thing Admiral Kime was most noted for was his openness and his invitation to the private sector to influence how the government and the Coast Guard did its work. That will very much be his legacy in the Coast Guard, and I think there are many principles that we draw on today with the public-private dialogue across all the sectors. So I note with sadness Admiral Kime's passing and I celebrate his government career.

Another person I would like to introduce today, new to the CIP Program, is Jeanne Meserve. Jeanne comes from CNN, the Washington-based America bureau, a unit that combines the network's homeland security, Justice Department, and national security beats to examine the state of security in the United States, a very unique combination. One of the things that was very exciting when we started to talk about working together is that Jeanne takes a very multi-disciplinary approach to her work.

Covering homeland security since September 11, 2001, Jeanne has reported on security at the nation's ports, the chemical plants, airports, and borders. She's had a more exciting career than I had in the Coast Guard. She flew with a federal air marshal. She accompanied an air combat patrol in an F-16 and stood atop a 13-story crane at the port of Los Angeles. And now, she's jumping into the shark-infested waters of academe, so this is interesting.

Jeanne's been the recipient of numerous awards and has been repeatedly recognized for her outstanding work and particularly her passion and commitment to getting the facts right, so we welcome her to the CIP Program and we very much appreciate her leading this discussion today. (Applause.)

Now, to introduce our guest speaker, in your package, we put a bio. One of the two things common in Washington are PowerPoint slides and reading people's bios. George Foresman has one of the most impressive pedigrees that anyone in the Department of Homeland Security can offer. He's seen it from all levels of government. He's seen it from a tactical view. He's seen it from a strategic view. And that's the combination that I personally think is needed right now. So I won't bore you with the details.

What I'd like to say is something that probably he doesn't hear a whole lot, and that is thank you. Thank you for your public service. I know personally that you had choices, and that you chose to serve the nation, and that there are days when you go home and you feel like you're getting it from all sides, including your own. But that's part of the game and we very much appreciate your service and for standing up and taking the bullets. Thank you, George. (Applause.)

GEORGE FORESMAN: Well, I'm going to very much thank John for that introduction and very much want to acknowledge the work that John has done at the George Mason School of Law, and the work that he's done on critical infrastructure. John and I go back many, many years and we were actually talking about critical infrastructure and dealing with critical infrastructure issues long before it was the norm and in the lexicon of most of America. And John, I very much appreciate those kind comments.

I will acknowledge, though, that as he was going through those and he was talking about taking bullets, I was reminded of the fact that I have a little practice that I do when I get up in the mornings. Usually, my six-year-old son who likes to get up early in the morning will race into the bedroom and say, "Daddy, what are you going to do today,"

and this morning was no different. At 5:00, he was up, which just made his mother exceedingly happy.

About four weeks ago, I went over and spoke to the Society of American Military Engineers, known as SAME. And that morning, my son had said to me, “Daddy, what are you going to do today?” And I said, “I’m going to give the SAME speech”. And he said to me at that time, “Well, Daddy, don’t you think they’d like to hear something different?” So this morning, Ryan came running in, jumped up on the bed, and said, “Daddy, what are you going to do today?” I said, “I’m going to give a speech.” He said, “What speech are you going to give?” I said, “I’m going to give a CIP speech.” He said, “Don’t people already know how to drink in this town?” (Laughter.)

I am very much appreciative of the opportunity to spend a little bit of time with you all today, and also to acknowledge once again the work that George Mason has done. John, I will echo your comments about Jeanne Meserve. Jeanne is a member of the press whom I’ve had the privilege to work with over the course of my many, many years both in state government in Virginia as well as being on the other side of the camera from her in this current job in the federal government, and she does put a high premium on understanding the issues and reporting the issues accurately and succinctly. And I think that we are well served as a public when we have the press out there telling the story and helping the American people to understand what the policies are, what the policies are going to be, and what their input into the policy process should be.

You know, I’m particularly pleased to be able to talk today about private sector challenges including the critical challenges that we face in protecting the nation’s infrastructure because I think more so than ever, we recognize in the aftermath of 9/11 and the aftermath of Katrina, the stakes for both the public sector and the private sector as it relates to our ability to provide for security in America, our ability to protect our critical infrastructures, have frankly never been higher.

And, you know, we spend a lot of time talking about a wide range of issues on homeland security, and sometimes, in those wide ranging issues, we don’t spend as much time talking about critical infrastructure issues and talking about the unique policy challenges that government faces, that the private sector faces, those things that are going to confront us in the 21st century.

All of us know that we are in fact engaged in a war on terror. As a nation, we have recognized the importance of defending our private sector assets from a wide variety of attacks. I was up on the Hill a couple of weeks ago. We were talking about cyber-security; we talked about physical security. And we understand that when we talk about protecting the nation’s critical assets, it is not a single thing that we do; it’s a multitude of things that we have to be able to do together.

And when we talk about the war on terror, we see our focus on critical infrastructure is reflected in the president’s national strategy to combat terrorism. I know it’s reflected in what I hear when I travel around America. And one of the great things

about coming from the state side is I spend a lot of time with the nation's governors. And the nation's governors are in fact concerned about what are they doing to protect their citizens, what are they doing to make sure that their ports are viable and operable. But governors are also absolutely concerned about what is being done to protect the business and the economic interests in their states.

And I also know that in the job as the Under Secretary for Preparedness, being able to work with very many talented men and women in our infrastructure protection division, under the leadership of Assistant Secretary Bob Stephan who is doing a wonderful job, I know that when I talk to CEOs – I had a CEO in yesterday of a major national corporation, tens of thousands of employees – and I talk to CEOs of small businesses, 10 or 15, and they are concerned about what should they be doing; what are we doing at the national level; what are states and communities doing to ensure the protection of their critical businesses, their critical infrastructure. And most notably, I see this as a beginning of a dialogue among the American public.

Most of you know that I came to this job from Richmond, and when I chose to come to this job, Gail and the children came up to Washington with me, but we kept our house in Richmond. And we go down there, and there is a group of individuals who I kind of consider thought leaders. One of the guys is a woodcutter; the other is a farmer. One of them I've never really figured out what he does, but he seems to have a lot of money and is quite happy doing whatever he does. And these guys gather for coffee every morning in a little country store down the road from the house, and I frequently, when we're down in Richmond on the weekends, go spend time with them. And you know, in the days after 9/11, they wanted to know what the state police in Virginia were doing. They wanted to know what we were doing with the National Guard.

But I will tell you, that conversation has dramatically changed among those men and women. It is a conversation about how are we going to ensure the vitality of the banks where they put their money on a day-to-day basis? How are we going to ensure that the parts and the fuel that they need to be able to conduct business on a day-to-day basis show up where they're supposed to show up?

And so what I would say is that as we go through this education in America with regard to homeland security, as we go through this evolution with regard to infrastructure protection, we realize that the American public's understanding of the issue is growing more and more every day. And that's absolutely critical because it's going to be critical in the context of expectations that are being set for us in government, and the expectations that are being set for our private sector partners as well.

You know, shareholders are awfully concerned about making sure that they get the best return on their investment, and corporate CEOs have to be concerned about that. And so, they want to know that the private sector is managing its risk as well as government is managing its risk. And I very much will say to all of us, the expectations that we have from a governmental perspective have never been higher. The lessons that have come out of Hurricane Katrina, the lessons that have come out of 9/11, the lessons

that have come out of the recent British airline plot – the American public expects us to do well and to do better in government, and we are committed to that. But they also expect us to do well and to do better as it relates to the private sector.

But one of the things that we clearly learned from September the 11th is that the costs associated with a terrorist attack are extremely high. You know, when you look at the losses that occurred in the immediate days and months after 9/11, there are some startling figures – 83 billion (dollars) in total losses including more than \$2.7 billion to the New York/New Jersey metropolitan area in 2001 following the 9/11 attacks. A significant drop in the number of New York companies that were able to raise venture capital funds, they fell from 46 percent in the last quarter of 2001 to 17 percent in the first quarter of 2002. And I think that these numbers are just two small indicators of how devastating a major attack or series of attacks or catastrophic natural disaster could be to our country, how devastating they could be to our economy, how devastating, frankly, that they could be to our way of life.

I, like many of you all, watched from afar as the events with Hurricane Katrina unfolded. And Jeanne is one individual whom I know was right down in the middle of the events down there. We spent much of our time focused on how were the rescues going to occur to take people off of rooftops; how were we going to get critical relief supplies to people who were in shelters?

But on the backside of all of this, there were a lot of unknown things that were going on as it relates to America's critical infrastructure. You know, the one statistic that I always tell folks is on the day before Hurricane Katrina, 25 percent of the nation's petroleum production occurred in Houston, Texas. The day after Hurricane Katrina, 47 percent of the nation's petroleum production occurred in Houston, Texas, because of the amount of refineries and capacity that was taken offline in Louisiana. And so that what we very much understand is, whether we're talking about terrorist attacks or whether we're talking about natural disasters, whether we're talking about a catastrophic earthquake in the L.A. Basin or the New Madrid Fault, we understand that the economic consequences for America can be exceedingly high.

And we also understand that our economic security and our national morale, and frankly the health and welfare of our citizens and the nation's security are dependent on the stability of our private sector partners. While much attention has been focused on the performance of government, we clearly understand that 85 percent of what we are trying to protect here in America is in the hands of the private sector. Government has a clear role in protection, but, ladies and gentlemen, let me be very clear; it is not an exclusive role. It cannot be an exclusive role, because government lacks sufficient resources to be able to protect everybody and everything all the time and everywhere. And so, it requires a collaborative partnership, and that's a large part of what we are focused on inside the Department of Homeland Security, the role of the federal government, state government, local government, and the role of the private sector, and most importantly, the role of the American people.

As we saw in the months following September the 11th the attacks that we saw on that tragic day had severe economic consequences beyond New York and Washington, D.C. You know, when we look back at the statistics on a national scale, we know that the stock market dropped by 12 percent by September 21st. Jobs fell by 943,000 in the last three months of 2001. And the information technology sector lost nearly one-fifth of its workforce.

Now, there are those who will say that we were headed towards some level of economic downturn prior to the 9/11 attacks and they are correct. But we also know that the 9/11 attacks clearly exacerbated what was our current economic situation in this country. And for as horrendous as they were, we understand that they could have been significantly worse had it not only been in Shanksville, Pennsylvania, or in New York City or Washington, D.C. Had it touched on us in the mainstream core areas of America, in middle America, the West Coast, then those tragic effects that we saw, those significant economic effects we saw could have been much greater and much worse.

And we also experienced during Hurricane Katrina the understanding of our dependency on critical infrastructure. You know, so much of our response at the federal level and the work that Louisiana, Mississippi, and Alabama did was dependent on restoring critical infrastructure services. These services, including water, power, and communications all support fundamental human needs. However, these services also depend on a robust and reliable supply chain, which played an integral part in the hurricane recovery effort. Multiple critical infrastructure services operated by the private sector regularly ensure the effective functioning of the supply chain, including our airlines, railroad, trucking, and shipping.

And the one thing that I intuitively understand – and I've been in this business for a quarter century – is this, when you talk about response in a community and when you talk about recovery in a community, it begins when you open the first business and you restore the first piece of critical infrastructure. We can pour in plenty of relief supplies in the aftermath of an event. But until the lights come on and the telephones are operating and the stores are open and people can run down the street and get a little bit of food or a little bit of fuel, you don't start recovery in a community. And when you don't start recovery in a community, you cannot start recovery in a nation.

And finally, we also know that the public and the private sectors are connected and interconnected by business relationships and technology. While our nation's critical infrastructure encompasses many distinct sectors, we must remember that these sectors operate within complex relationships. The sustainability of one sector depends on the security and the reliability of others, which was demonstrated on a large scale after September the 11th. For example, although 9/11 most significantly impacted the telecommunications, the banking, and the transportation sectors, the attacks also had an indirect impact on other critical infrastructures such as medical facilities and the hospitality industry. We know that there were nearly \$800 million in economic impacts to hospitals and healthcare providers through 2003 as a result of 9/11, and \$8.3 billion in cleanup and hotel replacement costs.

Problems with response and recovery operations after Hurricane Katrina also revealed that critical infrastructure sectors are mutually dependent or interconnected at the highest levels. Following Hurricane Katrina, a prime example of the critical infrastructure dependency came from the communications sector. You know, our “Federal Response to Hurricane Katrina: Lessons Learned” report that the White House completed pinpointed specific problems experienced by infrastructure owners in restoring communications services. The report additionally described interdependencies between critical infrastructure sectors such as energy and transportation that impact the restoration of critical communications services. In short, what that means is that when the power went down for an extended period of time, our telecommunications sectors were unable to operate. Some had backup power; others didn’t. Others needed to get replacement equipment in and they lacked the resources to do it.

And Katrina was a vivid reminder that there is a natural relationship, and, frankly, a natural partnership that has to exist on the tactical level between the public sector and the private sector and on a strategic level between business and government as a whole. And by that, I mean, it’s the ability to be able to provide resources to clear debris, to restore power lines, to then start up the telecommunications sector. It’s the ability to use critical assets to move resources into a disaster impact zone so that you can restore telecommunications or electric infrastructure. It is the ability to understand that if we close the nation’s ports for an extended period of time, it has a dramatic impact on the nation’s supply chain.

But these interconnections make the challenge of securing our critical infrastructure in the nation phenomenally challenging. And I’ve got to tell you, we deal with a lot of issues. We deal with grant issues every day; we deal with information-sharing issues; and those are complex and they are tough issues. But among the toughest issues that we continue to deal with as a nation is how are we going to protect the nation’s critical infrastructure? What is the role of government? What is the role of the private sector? Where is there the ability for collaboration?

And while we recognize the realities of these challenges, the federal government knows that it cannot instruct the entirety of the private sector on how they should best manage their security challenges because we realize that they own many of their security challenges. But we recognize that their security challenges are part of our national security challenges. And both entities, government and the private sector, must arrive at a shared end-state and we know that our paths to that end-state will, for a variety of reasons, differ. And that’s okay, as long as we arrive at the same destination.

Ladies and gentlemen, we’ve spent a lot of time talking about protecting the nation’s critical infrastructure, and we’ve spent a lot of time talking about the challenges that keep us from protecting the nation’s critical infrastructure and further strengthening the work that we’ve already begun. But we have got to change the dialogue. It cannot be about what is preventing us from progress, but it’s going to have to be about what is empowering us for more and more progress on a day-to-day basis. Every company and

institution represented here today appreciates the importance of preparedness. You have legal reasons for it; you have economic reasons for it; and all of you all are good Americans and you have great national reasons for it.

In my experience as an emergency management professional for more than 22 years, I have a high regard for the private sector's focus on customer service and reliability, as well as business concerns such as protecting earnings and reinforcing shareholder confidence. However, today, I would like to address those risks that transcend current business continuity strategies.

No single company, no sector of the economy, or even the private sector as a whole can address the realities of catastrophic risk without new levels of public sector and private sector collaboration. My focus today is instead on institutionalizing a preparedness system both in the public sector and the private sector for incidents that transcend the current public and private sector capacity to deal with the routine, those emergencies and disasters that we are struck with on a day-to-day basis, and we are able to deal with, and to make sure that as a nation, we are truly ready for catastrophic events.

It's hard to imagine disasters that would result in long-term power outages, disruptions of the national supply chain, or an Internet failure for over three months. These disruptions, while less likely, could occur after a massive natural disaster or a terrorist attack, so we must ensure that we take the lower-probability, higher-consequence event as seriously as we do the higher-probability event that we're confronted with on a day-to-day basis.

In that context, I would like to address three specific challenges facing the nation's public and private sectors. First, how can the government at all levels better communicate and coordinate with industry to manage catastrophic events? I know that each of you private sector representatives here today will speak to the need of closer cooperation. I also believe that communication will be one of the toughest impediments to establishing closer and more productive preparedness and response capabilities across this nation, and this includes both the boots-on-the-ground operational issues as well as the long-term strategies for fusing at the hip both public and private sectors in the context of our physical effort as well as our economic efforts. Both in my personal and professional experience, I have been reminded time and time again that without consistent and accurate information, communication with those around us is going to be nearly impossible.

And let me just digress for a moment, and I want to drive this point home. When I moved to northern Virginia, people said to me, if people ask you what you do, just say "I work for the government." I learned that. Well, I got into the house where my wife and I are living, and a neighbor came over and said what do you do? "I work for the government." He said, what do you do? "I'm a consultant in the beltway." What area do you consult in? "Homeland security." Well, who do you work for in the government? "Oh, it doesn't make any difference." (Chuckles.) He said, well, are you in intelligence; are you in defense; you know, what are you doing? I said, "Well, I tell you what" – I was

just trying to break off the conversation – “you don’t have to worry unless a helicopter lands in the front yard. If a helicopter lands in the front yard, we’ve got a problem. Other than that, things are good.” I didn’t know where I lived in Fairfax County that the MEDEVAC landing pad was right across the street from my house. (Laughter.)

So about three Saturdays after we move up there, MEDEVAC comes in one Saturday night; I go out to get the paper on Sunday morning – all my neighbors are out there because I had not communicated with them effectively, and I’d left the wrong message. And folks, I use that as a little bit of a trite example of the importance of making sure that we have open, honest, clear, and effective dialogue and communication about what are our expectations; what are our needs; and frankly, what our capabilities are.

And for me, that experience highlights that the communication challenges include not only what to communicate after a disaster, but how to communicate in advance so that we are prepared at a very sophisticated level. For example, not all corporate executives sufficiently understand how the government prepares for and responds to catastrophic events. We in government must do a better job of educating senior decision makers who are largely responsible for employees, corporate strategies, supplier and vendor relations, and shareholder confidence. We need to educate them about what we’re doing so that they can educate those who work for them and who depend on them and who are shareholders to them about what we are doing.

Catastrophic events threaten each of these key corporate areas, so ignoring government authorities and plans is not an acceptable solution. Government cannot bury its head in the sand; corporate America cannot bury its head in the sand. We must work collaboratively. But by the same token, government is unable to manage catastrophic events without harnessing the full value of our relations with our private sector partners.

Clearly communicating our respective rules of the road, our strategies for preparedness and response, and our needs are all conditions for success and overcoming the communications challenges that we face. One area that requires special attention from industry is in fact the National Response Plan and the authorities that support the execution of this emergency framework. The federal government is currently in the process of making major updates to the National Response Plan. It must be more robust; it must be more integrated; and it must be more filled with an understanding of our complex relationships between government and the private sector and the National Response Plan must reflect what government needs to be able to do in consonance with the private sector to deal with catastrophic events.

Clearly communicating our respective rules of the road, our strategies for preparedness and response, and our needs are conditions that will be critical, as I’ve said. As we update the National Response Plan, we know that it will be an update based on the plan needing to be an idea that incidents are typically managed at the lowest possible geographic and organizational and jurisdictional level, and that incident management

activities are initiated and conducted using the principles contained in the National Incident Management System.

The reason that's important is the decisions that we make at the federal level will be executed at the local level. And while we need to make sure that there is a relationship between the federal government and the private sector, we also need to make sure they are equally strong relationships between the private sector and local and state government, and they will follow in that context behind what we do in the National Response Plan. The overall goal of the National Response Plan is to provide the structure and mechanisms for national level policy and operational direction for domestic incident management for all hazards. The National Response Plan is not a natural disaster plan; it is not a cyber plan; it is not a terrorism plan. It is an all-hazards plan that will serve us well in any event.

Secondly, I believe that most communications challenges stem from the lack of a shared vision for preparing and responding to catastrophic events. The challenge we face then is clearly defining and participating in a shared vision of catastrophic preparedness both in the public and the private sector. This second challenge goes to the core of the divide between the public and private sectors. Even more refined communication and coordination will not deliver a shared vision and clear expectations. The horrific attacks that took place on September the 11th provided a fundamental opportunity to seize this teachable moment and lay the groundwork for a national approach that integrates prevention and protection with response and recovery. Hurricane Katrina showed us that despite 9/11, we continued to lack an integrated national approach for managing the full range of risks that we face.

But let me be clear: We are making progress. From a governmental perspective, we have taken important action to respond to the White House, the Senate, and the House of Representatives after-action reports. These three reports yielded a combined 224 recommendations. The department has used these recommendations to identify the critical actions to be accomplished in advance of the current hurricane season, and we got those done, as well as those that need to be conducted over the course of the next weeks and months. Secretary Chertoff and President Bush have made the accomplishment of all of these after-action actions top priorities and are holding people accountable for progress.

The private sector, states, and communities in America do an exceptional job every day in dealing with the vast majority of emergencies. However, in the aftermath, the nationwide planned review requested by the Congress and the president demonstrated that at least in the public sector, we are not where we need to be as a nation with regard to our shared responsibility to manage catastrophic events. That shortfall should not be construed in any way to reflect a lack of dedication on this effort. But rather, it reflects the lack of a shared vision for truly how prepared we need to be individually and collectively as part of a shared system for our comprehensive national approach to preparedness, which would focus our efforts and provide standard tools and processes to

get us there – all levels of government – local, state and federal – as well as between the public sector and the private sector.

So at a minimum, the public and private sectors should undertake a new covenant to deliver a shared vision for generations to come. Ladies and gentlemen, we have a teachable moment if we choose to grab hold of it.

While such agreements have traditionally been viewed as contractual, I use the word covenant to clarify my expectation and our expectation for a shared public and private sector vision. The word covenant means to come together. And in this sense, I use covenant to signify that our shared vision must be steeped in deep notions of trust, respects, and clarity of vision.

In turn, the term partnership is quite often used to refer to our public private interaction. But I believe that we must first recognize our respective visions – that we must first recognize our respective visions and then come together with new strategies, new relationships, and new commitments.

A shared vision for a catastrophic event would embody several principles and these would be shared, coincidentally, across both government and the private sector. First is a deep concern for the loss of life. Second is a deep respect for public trust and confidence, whether in our institutions, our economic markets, or our way of life. And third, recognition that the public and the private sectors share common risks, including threats and vulnerabilities, and thus we all share in a common responsibility.

Finally, this covenant would acknowledge that the management of catastrophic events will not be easy, but the risks of going it alone or not doing anything are simply not acceptable. The American public expects more; the American public deserves more.

Third, if we are able to communicate and to come together with a shared vision, what are specific short- and long-term solutions that merit prioritization? In a meeting with leaders across the nation, one challenge more than any other will demand our attention: integrating our plans to account for catastrophic events. As I alluded to earlier, each and every representative on this panel has sophisticated preparedness and response plans in their own businesses. We proactively exercise these plans. We train and educate our people. We audit our suppliers and we use other tools to promote our institutional responsibilities. But companies and government agencies must socialize our plans into a collective framework. To accomplish this, we must become comfortable with several concepts and protocols.

First, the private sector must compete on market principles, but collaborate on security needs. Second, government at all levels must find new ways to bridge jurisdictional boundaries so that we can harness the power of our skills and services. And three, both public and private sectors must set clear expectations and negotiate these expectations so that plans and protocols are integrated into a single national approach.

Ladies and gentlemen, achieving these goals in our busy lives is not going to be easy. But I've had nine months to reflect on 22 years at the state and local level working in partnership with the private sector in Virginia, and I will tell you, there are a couple of clear takeaways from this nine months. The first of these is that this is tough. It is a phenomenally tough challenge to find the right environment where the old modicum of government being the regulator and the private sector being the regulatee, where you overcome that cultural institution to create true collaborative partnerships that promote preparedness.

The second challenge that we face is that we do speak different languages. I've worked for five governors in Virginia, Republicans and Democrats. It was always interesting. Every governor came into office and they reached out to all of the graybeards, the gravitas in the business community, and said to them, come in and tell us what we can do to improve our operations, our customer service, and state government. But it was always interesting because the private sector would come to the table with the public sector, and we don't speak the same language. And that's okay. But what we do have to do is find a way to translate our needs and desires in government and the needs and desires of the private sector into a common language.

And third and finally, we have to understand that at the end of the day, beyond all of the motivations – and I hear all the discussion about how government doesn't operate to make a profit; government operates to provide critical services to the citizen. Businesses operate to make a profit; businesses operate to grow. I understand all of that. And those are very different shared approaches to the work that we're doing. But at the end of the day, traveling all around America, I've not found one person that doesn't want a safer and more secure America. They've said they want a safer America in the context of their physical security, their economic security, and the stability of our society. Not a corporate leader has told me that they don't want that; not a government official has told me that they don't want that; not a citizen of America has told me that they don't want that.

And so, what I would offer to you all today is that we have an opportunity in the post-Katrina environment, in the post-dustup environment of a whole lot of things, to recommit ourselves to this public-private sector collaboration and to recommit ourselves to truly working through these challenging issues, because I've got to tell you, something is going to happen. It may be tomorrow. It may be next week. It may be next month. And if you're from government, your citizens will expect performance. And if you're from the private sector, your customers and your shareholders will expect performance. Our job is to make sure that we deliver on those expectations. Thank you very much.

(Applause.)

JEANNE MESERVE: I can't tell you how many times since Hurricane Katrina I have heard from officials and experts, "Well, there's absolutely no way we could have been ready for that," as if that excused the lack of preparation or the tragically flawed response to that catastrophe. The fact of the matter is we're supposed to be prepared for

that kind of event. If you look at the national planning scenarios that are supposed to guide our preparedness efforts, they talk about terrorist events and natural events, which could cause casualties in the tens of thousands, the evacuation of millions of people, billions of dollars worth of economic damage, and that require years to recover.

So of course, the question we hope to address today is how do we get there from here, particularly looking at this public-private interface, talking about where there are gaps, where there are redundancies, where there are conflicts, where there is room for collaboration, and that's where we'll go. I'm going to quickly introduce our panelists here today, and I'm sure my very quick introductions will not do justice to their expertise and experience, so my apologies in advance. But we want to get right down to the meat of the discussion.

First of all, Paul Kurtz is here on the end. He's the Executive Director of the Cyber Security Industry Alliance. Previously, he was on the Homeland Security Council and the National Security Council, where he dealt with cyber security issues.

Immediately to my right is David Noznesky. He's Director of Corporate Security at Florida Power & Light Company. His organization weathered the first World Trade Center bombing and learned early about the importance of being prepared and having a continuity plan in place.

To my left is David Eisner. Mr. Eisner is Chief Executive Officer of the Corporation for National and Community Service, which is an independent federal agency that administers the Senior Corps, AmeriCorps, and other volunteer organizations. They try to provide strategic support to volunteer organizations with the goal of making them more effective. He and his organization are involved in the Katrina response.

Next to him is someone else also very deeply involved in the Katrina response, Johanna Schneider. She is Executive Director of External Relations at the Business Roundtable.

And finally, last but not least, Harry Oellrich. He is Managing Director and head of the Cyber Technology and Intellectual Property practice at Guy Carpenter Insurance. He told me that insurance companies are among the economic first responders in any catastrophe.

I am sure that I have not said enough about the experience each one of you has had in this area of infrastructure protection and disaster response. So I'd like to start out by asking each one of you to talk a little bit more about what you bring to this conversation, but also to look ahead from here, where you think we should be in 10 years and what are the real strategic obstacles that have to be overcome. Paul, I'd love to start with you because you said to me on the phone that you didn't think the government would even know if a cyber attack was underway quite possibly.

PAUL KURTZ: I'd be happy to start off. And first of all, I wanted to thank the Under Secretary for his remarks. And I think the piece I might bring to the table is that I agree with everything that the Under Secretary set out today. I think they're all very important statements of the government's approach to the problem, philosophical and aspirational. And I think many of those same statements were made several years ago. In fact, I made them; others have made them in the past. And I think where we ought to be going is into hard priorities and hard programs. And I think one of the things that troubles me is we're not able to go through and identify hard priorities and hard programs that affect the protection of all the key infrastructures across the United States.

And that's not to say that the Department of Homeland Security is not doing anything. In fact, I think George and others could talk about the CIP grant that has been given to cities and municipalities to help them shore up their information infrastructure. But we should be moving to a place where we're talking about the programs that have been set up and, if you will, debating whether or not those are in fact the right programs – kind of, if you will, if you look at where we are with DOD, we debate about what kind of aircraft we should have for the future. Does that impact the light aircraft in our defense? We are not having those very specific debates about programs and critical infrastructure protection. And we need to get there sooner rather than later. I would argue we've largely been running in place. We've had some progress, but we need to get more specific about what we want to do in the future.

MS. MESERVE: Great. David?

DAVID NOZNESKY: Well, I heard Under Secretary Foresman and actually took some very profound things relating to public-private partnerships. Having come from both sectors, the private and the public, they really do have a hard time talking to each other, and in fact, not only did they not speak the same language, but for some reason, culturally in the government, it's very difficult to speak in that language to the private sector.

But I think some positive things have happened in that partnership. First, for a challenge, our industry, in particular, Florida Power & Light Company, is well versed in disasters and the challenges that they present. So culturally, we know that those relationships with the state and local governments and the federal government are critical before a disaster. And if there's one thing that I could say to the two companies is that in business, continuity planning, it is absolutely critical to develop those relationships and those dialogues before.

I think for corporate security officers today, one of the biggest challenges today is business continuity, crisis management, and certainly 9/11 brought a whole new focus and dimension to what is business continuity. And I think in the area of improvements, I think we've seen recently the development of the National Infrastructure Protection Plan and also the private sector specific plan has done a lot to improve the partnerships between our industry, and the input our industry has had with the Department of Homeland Security.

So I think strategically, those dialogues have to continue; those relationships have to continue, and that will be a critical part of being able to continue and be resilient. Undersecretary Foresman said you can't protect everything everywhere every day, and of course, in our industry, that's critical, because you have to be resilient. You have to have good restoration planning.

MS. MESERVE: David Eisner, you come at this from a very different perspective.

DAVID EISNER: Yes, well, in addition to now being at the Corporation for National and Community Service, during 9/11, I was at AOL Time Warner – managed this from the corporate side. I think that the thing that I'd like to make sure we're able to focus on better is the connectivity between the need and the opportunities that companies and people have to fill those needs.

In Katrina, we just saw over the last year 575,000 Americans volunteer in the Gulf. And it was literally in the billions of dollars that companies were providing in cash and in-kind support. But what we found over and over and over again is that in spite of the incredible need, and in spite of people and companies' willingness to fill that need, that we didn't have the capacity. There was no capacity to use the resources that were being provided.

So over and over again, we'd see a town that was devastated that needed support to bring its power back online. There would be power companies that would be willing to send people and support into that town, but the town administrators didn't have sufficient capacity to even enter into the dialogue about how to get those other companies to bring their philanthropic support to bear.

So I think that this is really about, first of all, making sure that we have the relationships. The Under Secretary spoke compellingly about the need for communication. I actually think it's about people-to-people. It's about relationships. In the heat of the moment, it's very, very hard to learn to speak each other's language, and it's very, very hard to make offers if you don't know each other. We found that the organizations and the communities that really leveraged these resources, the best were the ones that had the pre-existing relationships between people.

MS. MESERVE: Johanna?

JOHANNA SCHNEIDER: First of all, thank you, George, very much for your insightful comments, and thank you, audience, very much for coming out on this very, very important topic. The Business Roundtable is an association of CEOs of America's largest companies.

And to answer your question, where would we like to see things in ten years, we've looked at this from all angles. Our companies were very generous in the

immediate aftermath of Katrina in trying to help the nation recover – first, save lives obviously, but secondly, try to recover as quickly as humanly possible. The lessons that we learned were that to really impact things in the future, we needed to organize ourselves most effectively, first and foremost. We needed to be able to provide to the government an integrated business community so that when the government needed us or when there was a catastrophic event in the United States, we were able to bring to bear all of our full resources.

So what we're working on – and we may get into this further – is trying to leverage our own company strengths, our own cross-industry disciplines, so that when there is a catastrophic disaster – again, to George's point – there's never a routine disaster, but there are certainly issues that are so catastrophic, you would expect the corporate community to bind together and to be able to respond as one.

One of the problems that we identified in 9/11 and in Katrina was you had the tendency, as government, to try to identify and pick off, so to speak, businesses that A, you're familiar with, or, B, have come to the fore in the past. We need to be able to provide to NGOs, to the government, a united front, so to speak. So business has already done the hard work of educating our employees, our CEOs, and all of our senior executives – and then, preparing, drilling, and being ready when a catastrophic disaster comes to bring to the table a very specific set of resources that we can provide to assist in a national recovery plan.

MS. MESERVE: Harry, I think all of us probably turn to you if there's a crisis.

HARRY OELLRICH: Well, I do view us in some respects as analogous to first responders in a tangible sense in that when bad things happen, basically you look to either government or to the insurance and reinsurance industry to maintain or to preserve liquidity. And I think that's something that gets lost in the translation in much of the debate that goes on relative to whether our sector's companies are doing what they should be doing, doing all that they should be doing, et cetera.

Maybe I should back up a bit before I move forward though and just indicate – because I think what I do for a living is slightly less intuitive than some of my colleagues here on the panel. I represent a firm by the name of Guy Carpenter & Company. We are reinsurance, not insurance brokers or intermediaries. Our clients are the major insurance companies worldwide. All insurance companies, from the smallest single county mutual, right on up to the major multinationals basically purchase reinsurance to be able to manage their risks.

They specifically buy it in the context of today's discussion to protect against untoward or unacceptable accumulations or perceived accumulations of catastrophic exposure, be that to earthquake, to hurricane, to cyber, to a whole host of other events, both known and unknown. And really, to be able to get insurers to play that role and to play it to a greater extent – reinsurers to sit above them and support them – we really need to be in a position in ten years to be able to be working very much more closely

with everyone who is a stakeholder in this debate, everyone who has a horse in this race, in that we don't have all the answers.

Our industry has basically spent the last decade or more reaching out, trying to develop some pretty sophisticated models to be able to try to sort out what our maximum foreseeable or probable maximum loss might be in any real or hypothetical event. And we don't have all the answers. The government has data that we probably can't even imagine if we could mine it or know where to turn to be able to work with them to mine it.

If we can do that, if we can build even more sophisticated models that will help to provide insurers and reinsurers with additional confidence that they can figure out what their loss could be by entertaining certain exposures, they'll write more. Or maybe they'll write a lot of those exposures and over time, we build out a much more sustainable and long-term and robust market that can also basically help to harden infrastructure in and of itself because what it does, it will basically create best practices, if you will, that an individual firm or an individual would need to be able to have to be able to either afford coverage or to be able to procure coverage in the first place. So we think that we can play a fairly prominent role if we're able to work even more closely with government than we have in the past.

MS. MESERVE: One of the comments here has been communication, both from the Under Secretary and all of you. But, do you even know who to talk to? Is it clear who in government plays what role, what their responsibilities are, who the go-to people are? Why don't we start with you again, Paul?

MR. KURTZ: I think the answer is yes and no. I think at an everyday level – let's get specific – in the IT community, there are a set of points of contact that the private sector can go to at the Homeland Security department to talk about IT issues.

I think where it gets more interesting and of greater concern is what happens if we have a more significant event where we've graduated from the noise of every day. We have something going on in the networks that it requires more senior level attention around government, not just at the department of Homeland Security, but DOD, the FCC, on up the line. You get into how do we do command and control during a crisis when it involves the IT infrastructure, and the communications infrastructure? I think there is not enough clarity as you escalate up the line as to who the real decision-makers are as we go forward. And I know the BRT's report has talked about getting into recovery and reconstitution issues – that's where we have some real gray area that we need to clarify roles and responsibilities as we get into a crisis.

MS. MESERVE: Johanna, you mentioned to me that you not only, of course, have to interface with the federal government but you also have to play with the state and local governments as well. How do you effectively do that when you've got a private sector that represents thousands of industries with things to offer? How do you communicate?

MS. SCHNEIDER: Sure, well, the long and short answer is it's a work in progress. Really, there is no one place to call, to pick up the phone. There is no 1-800 number to call for a variety of companies, for industry, for commerce. What the Roundtable has tried to do, and our companies have asked us to play this role, and we will see if we're effective and successful, is to essentially be a broker – to allow our companies to call us and for us to triage calls to the federal, state, and local.

We're undertaking an effort to work with the Emergency Operations Centers, which, as you know, are the key component in each state. Every disaster, every catastrophic event happens somewhere, as George said in his speech, and that somewhere usually has boundaries, has state officials, has a governor. So we are trying to do both – the bookends. We're trying to make certain that the federal government understands that we're a resource and we can be accessed for companies to get information from the federal government, but also to go to the state and local. I don't know that you'd ever find one 1-800 number to call, but certainly you can identify at least three or four areas of the most pertinent information.

MS. MESERVE: David, I'm sure you ran into that to a certain degree, but you also were in a situation where perhaps you had relationships with the Department of Homeland Security, and all of a sudden you found the Department of Defense was a key player.

MR. EISNER: That's right. And actually, there was a point at which the Department of Commerce very usefully stepped in and did come up with an 800 number that all companies could call, because up until then, it had been so fragmented and a lot of companies were feeling that they were offering literally in some cases tens of millions, hundreds of millions of dollars of product, and there was no way to connect. So the Department of Commerce did step in there. But still a lot of work needs to be done, and I think that the idea of interfacing through a business coalition works really well.

I'll also note that for a lot of volunteers, they also were frustrated. And although there were really powerful places like volunteer.gov and 1-800-VOLUNTEER and the Hands On Network for them to go, it was still very, very frustrating for folks that wanted to help and had an opportunity to provide really meaningful support, to actually get into the Gulf, to be able to deliver that.

MS. MESERVE: So the government had no way to leverage what you had offered?

MR. EISNER: We did not have either the relationships or the systems in place to be able to make the connection. I tried an experiment that failed dramatically.

MS. MESERVE: You shouldn't admit it, strategically or otherwise!

MR. EISNER: Well, you know, we all did. We tried to set up a warehouse, a clearinghouse where we had 20 full time people trying to take requests from the groups of folks that wanted to go down and offer assistance and connect them. That group was in DC, and we quickly learned that without having a similar group in the Gulf itself, actually doing the programming, we couldn't make the connection work.

MS. MESERVE: You were nodding also on that leveraging issue.

MS. SCHNEIDER: Well, the supply chain deficit is the bottom line, and the question is our mantra – “Dwell on the solution, not the problem.” How do we find the solution to this supply chain if – and everyone said it – if FedEx or UPS can get a package delivered overnight, how can the Federal government not tap into the business expertise that is available, to enable a supply chain to work during catastrophic events. There are many more challenges than just delivering the package, but still the technology and the expertise exists.

So that is actually the challenge in front of us, is to try to create some kind of a loop so that during a catastrophic event, you can both identify the needs, but as you have very correctly identified, get what needs to be moved from the outpouring of support in America to the place where it's necessary--and not just to the tarmac. It has got to get off the tarmac, down the street, to the locale, because as you all know, far too often in a disaster situation, supplies sit on the tarmac, and they can't get to the actual location to save lives.

MS. MESERVE: Under Secretary Foresman mentioned this problem of language and people speaking in different tongues. I saw a couple of heads nodding when that conversation was going on. Harry, you were saying, yes, yes. How big is the problem? How does it demonstrate itself, and how do you do the translation?

MR. OELLRICH: We have tried to work on some of the specific issues that I have personally been involved with, with both the military, with government, and others within the private sector. And you find that aren't just two tongues; in many cases there are three. And when you put all of that together, it just becomes so much more difficult. When you compound that by all of the upheaval that has taken place regarding reorganization within the government, it becomes increasingly difficult within my own organization and within our sector to be able to make a business case to continue doing this.

And it became – when it started, it was basically a nights and weekends thing in addition to our day jobs, so to speak - but it really became very difficult to make a business case to spend as much time even as that with all of the changes that were going on. You would identify some individuals within government that seemed to get it, then unfortunately they would move on and you would have to start all over, and you might be successful; you might not be successful, but over a period of time, you weren't able to show the incremental progress that you needed to spend those kinds of resources.

It would be nice to have some sort of central point of contact that maintains some stability in terms of maybe not just an individual, but maybe a department or a unit within a department that would be identified as the go-to people for that particular issue or that particular subset of an issue.

MR. EISNER: I just want to note, I take maybe a slightly different vision. I actually think in many cases what is called a different vocabulary is really different cultures and that speaking different languages is actually a symptom of having different world views and different values.

Our constituency is made up of social-service providers in many cases, and we find that there is a serious challenge of respect flowing both ways between, on the one hand, the emergency management community and on the other hand, the social-service providers.

Social-service providers tend to look down on the emergency-management community as “guns, badges, and adrenaline,” thinking that they are all too top-down, too command-and-control, whereas the emergency-management folks will look at the folks providing social services as sort of fuzzy-headed, too consensus-oriented, not sufficiently focused on getting things done.

And so I think it’s important to understand that it’s not really a matter of communications or learning of vocabulary; it’s a matter of building actual relationships, and it is a matter of being able to respect each other’s job portfolio.

MS. MESERVE: David?

MR. NOZNESKY: I just want to say that we had talked about this difference in language, and I just can’t emphasize enough about the importance of having those dialogues, those discussions, those relationships before a crisis occurs. For example – and I know all of you can identify with this one – the lights go out; whether it’s a natural disaster, ice storm, hurricane, or whether it’s manmade; you want the lights back on. With the interdependencies that there are with various infrastructures, you know, it’s critically important to the economy.

So it’s not about having the incident occur and then having to rebuild; it’s a matter of knowing the expectations of our state and local partners, and also for them to know what we are going to do and how we are going to react, and that all goes to planning. And there are extensive plans, and our communication with our state and local partners is excellent. And, yes, we would know who to call and who to dialogue with.

Our industry, the power industry, is fortunate in that we have an organization called the North American Electrical Reliability Council, as well as the Edison Electric Institute. And they play a critical role in coordinating the activities of the major power companies or power companies’ grid operations throughout the United States, and that is our link back into the federal government.

So in those instances, in a disaster, we have really clear lines of communication, perhaps not one central 800 number or one department, but we know who to call to connect back through the Department of Homeland Security, or the Department of Energy to solve a particular problem to help expedite the issues.

MS. MESERVE: In part because your industry is called upon, on a regular basis, to deal with catastrophes large and small.

MR. NOZNESKY: On a regular basis.

MS. MESERVE: And so is your industry very much the exception in terms of having those channels, having those lines of communications already established?

MR. NOZNESKY: Yes, I would say it is an exception. But the lesson to be learned, again, are those critical dialogues before incidents occur, breaking down those language barriers, for example. On the law-enforcement side, on the security side in particular, those relationships are important with the FBI, the Secret Service, local and state law enforcement agencies so that when something does happen, first of all, your CEO, our CEO is going to want to know what is happening and how is it impacting our company, and so you need to be able to know who to call. All relationships develop over time.

MS. MESERVE: Paul, there are networks set up. There is the ISAC system where there is supposed to be trading of information between the government and the private sector. There is the Homeland Security Information Network, and so forth. Do these channels work? Are they able to overcome these obstacles that have been mentioned, these obstacles of language and cultures that exist?

MR. KURTZ: I think to a degree they work. And I think the IT sector is pretty interesting space. The IT sector has set up something called an Information Sharing and Analysis Center where members of the private sector have come together to exchange information. The IT sector has set this up at its own expense, if you will; it's not supported by the federal government, and it's been around for several years. And they have been able to develop protocols for sharing information. They have engaged in non-disclosure agreements so that they can share information securely.

What is problematic – there are two issues that I think manifest itself. First of all, the government has, if you will, kept the ISAC, this ISAC and I think others, not all, at arm's distance. And so – and to give you an interesting example, in the context of the London bombings last year, there were a lot of the ISACs that were wondering what in fact was going on. Did we have a problem here in the United States? What were we doing?

And a bridge was set up among many of the ISACs very early in the morning around 7:00 a.m. when news of the London attack came out. It wasn't until several hours

later that the department was able to come – the Department of Homeland Security was able to come out with its statement on what in fact was going on, but the private sector had in fact shared information in advance. They had started to develop the trusted communications channels and the lexicon in order to deal with each other during a time of crisis.

What I think is interesting also about the IT sector with regard to lexicon, when we have an event – and we will have an event, a large-scale event involving the IT sector – remember, geeks will be fixing the problem - that 99.99 percent of us will be standing on the sidelines because the software engineers, the enterprise architects – all of those people will have to be delving into the details, which means everybody else won't have a clue as to what is going on as people try to sort these out. And when the Department did its Cyber Storm back in February, one of the issues that came out of the after-action report was an issue of lexicon.

So you have senior people sitting around and all of the geeks are doing their geek talk, and they have to translate this up into what it means to the policymakers, what in fact is happening on the networks, what it means as far as response, and recovery. That is where I think exercises are incredibly valuable, and the Department should be commended for putting together the exercise. We need more of those on a more localized scale as well; they don't all have to be national in nature.

MS. MESERVE: What about pushing information up the chain, up to the Department, things that your industries or sectors may be aware of? Are you able to do that?

MR. KURTZ: I think to a limited degree, once again in the IT sector. I think in the communications sector, there is this bizarre bifurcation between the communications sector and the IT sector; don't ask me to explain why, even though we have convergence. Nonetheless, there is the IT sector ISAC, and there is a communications ISAC. The communications ISAC is in fact in a better space than the IT ISAC. Why? Because the communications ISAC is in part supported by the Federal government. The IT ISAC isn't. So you have more strained communications, if you will, between the IT ISAC and the Federal government.

And I think there is an honest effort on the part of the Department of Homeland Security to address those issues. And I think one of the important steps the department has taken is to put in place an Assistant Secretary for Cyber Security and Telecommunications who will be starting next week or the week after. And I think some of these issues will start to sort themselves out more rapidly than they have been handled in the past.

MS. MESERVE: Many of you have articulated issues that you have with this private-public partnership. Is the government paying attention? Is the government listening to your issues? Harry, I would really be interested to hear what you say about this.

MR. OELLRICH: I think that individuals within the government have taken the time to try to deal with what to many are somewhat arcane issues, but at the end of the day, how deeply that lends its way into the government is something that I'm not sure has really been proven. I said before, I think that many of the people that have worked the issues that I have been involved with have had to move on, have had to do other things, and therefore you have to start over again. And you make a little bit of progress and you go back, you make a little bit of progress and then you go back.

And in a dynamic business environment that we are in, we have to answer to our shareholders in terms of what we are doing and how we are spending our time, it becomes very hard to make the business case to be able to continue to do that.

MS. MESERVE: Paul, to take it back to you, there has been a lot of criticism on the cyber front for the government, that they just haven't been paying attention, they haven't grappled with it. Why do you think that is? Is it because they don't understand it? Is it because it's so large they don't know where to begin, or is there some other answer?

MR. KURTZ: I think those two reasons are valid. I also think it's fair to say that the Department has had some significant challenges since it started up. One, 22 or 23 agencies coming together is not an insignificant problem - all of those agencies with different cultures. Secondly, you can add Hurricane Katrina on top of that, which was obviously a very significant event for the Department, the Federal government, and state and local authorities.

Beyond that, we continue to have intelligence about attacks to the physical infrastructure, attacks that would kill people. When it comes to the information infrastructure, it's kind of hard to get your head around it. One, you can't really see it, you can't really smell it, you can't really feel it, but it runs everything, and so it's almost a feeling, if you will, of "it's too big to fail." It will always be there in some form or capacity, and those who say it may go black or something like that, or hype up the problem, you know, that in fact could happen. I think a more likely problem is that we'll have a loss in bandwidth issue.

But I think there has been a series of things that the Department has had to deal with, and this has consistently been on the bottom of the list. Now it's starting to move up. But let me put a marker down. I think today, this week, we have another potential problem in front of us. As the Congress is debating the reorganization of FEMA, the Federal Emergency Management Agency, there is discussion about having the cyber and communications division over on one section and FEMA over here, but having recovery and reconstitution rest within FEMA, which is essentially splitting out recovery and reconstitution from situational awareness and prevention efforts. It doesn't make a lot of sense.

When you look at an organization like the National Communications System, which has been around since the mid-'80s, they have had situational awareness and recovery / reconstitution together for a long time. And you could argue that is good. Now we may have the Congress rip it apart. That is not a good idea. It puts people like Under Secretary Foresman in a very bad position and puts the private sector in a nasty position of how do we – now, who do we call at the Department? Do we call someone when it comes to prevention and protection, and we call someone over here for response and recovery? It's not clear. We hope it shakes out properly.

MS. MESERVE: Well, the emergency managers are very excited about this legislation. They think it's going to bring more coherence to their world. Have any of the rest of you looked at this particular piece of legislation and thought about the implications for your sector? Johanna?

MS. SCHNEIDER: I think there are good changes and there are bad. You just put your finger on two of them. It was a mammoth undertaking. They have tried to do the best they can in terms of both positioning within the Department. The truth of the matter is your organization - CNN - is as much a leader in the event of a catastrophic event as any government agency, because information is king.

The fact of the matter is that what the government needs is to streamline the process of information, both pushing out and back. You just put your finger on an issue for the government, which is we want to get to the government; where do we go? But what about when industry has vital information that they need to communicate back into the government? That is something we are working on and we need to work better at it, but we need to be able to communicate to the government what industry needs.

MS. MESERVE: You can't do it now?

MS. SCHNEIDER: It's difficult. There isn't one organization that tries to corral business and provide across the economy a depth of information to what is necessarily needed within a 72-hour period to reconstitute commerce and to get the economy moving again, which in the event of any catastrophe, is absolutely critical, both for national security and for economic security.

MS. MESERVE: Harry, I wanted to delve into this insurance issue a little bit more. I think probably everybody here has some – wants to have some input in this discussion. You have explained how the insurance industry is a little reluctant to write this kind of coverage because they can't quantify the risks. Harry, you mentioned that the government may have data that could be helpful. What do they have? How do you think you can get it?

MR. OELLRICH: Well, this is really the \$64,000 question. There are so many different places within the bowels of government, so to speak, that data that could conceivably be directly useful, it could be used as a proxy for something that we might be able to build in conjunction with government, a model particularly in the cyber area. I

mean, we have a tremendous second chance here, and that, to Paul's point, it hasn't happened. It's likely that at some point in time it could happen, and, you know, it's very difficult to get insurers any exposure to cyber or bricks and mortar tangible exposures if they can't predict with some semblance of rationality what kind of a loss might result from a particular event. They are not going to be able to convince their board that it makes sense to be able to write very much of that exposure at all.

And because of that, if we can find a way to access things that government might have, individuals – the ISAC is great – they are more tactical. I'm thinking in a strategic sense, the ISACs deal with threats. I'm thinking about dealing with things that can physically be used to embolden insurers, to do more of these kinds of coverages, and by doing that, create those best practices. Like the factory owner that basically uses insurance. He needs to have insurance; he is told that he has to have insurance to be able to remain in business. He doesn't necessarily sprinker his factory because he is a nice guy or out of some altruistic virtue; he does it because he knows that he can't afford coverage or he can't get coverage at all without it, and without it, he is not allowed to do business. Well, very much the same thing can happen with other product lines that can, by definition, pull the entire infrastructure of the country up by its bootstraps by adopting those best practices.

MS. MESERVE: Paul?

MR. KURTZ: Yeah, I agree with Harry. I think there is a real opportunity here in the insurance phase when it comes to information systems to create an insurance market and to help industry handle some of the risk. And let me try to give you a couple of examples..

The Energy Policy Act passed last year puts in place cyber-security standards that the energy – the local electrical power community put together for itself; those are basically, if I understand this right, David, being ratified by the federal government right now. That creates an expectation on the part of the insurance community that there is a set of standards that electrical industry needs to meet with regard to cyber security. It is, if you will, a checklist or almost a certification that they are doing the right thing in this space.

That could enable ultimately the insurance industry to come in and say, look, I have an understanding, I have a certification that you're actually doing the right thing in this space, so we can come in and take care of the rest. It doesn't have to be a regulatory model though; it could be a voluntary model. You can take existing international standards, best practices for information security, encourage their adoption in the private sector, various parts of the private sector, and ultimately if the insurance industry has an understanding that a company is taking the following steps to secure and defend their systems along with resiliency plans, they feel more comfortable riding the risk.

I think government can add to this. Government can help create this market by stepping up and encouraging research, asking the tough questions. Commerce could get

involved in this effort as well. So I think there is a real opportunity here that has been sitting there for a few years that we haven't been able to capitalize on.

MS. MESERVE: David, I know you have said to me you don't want to see more regulation in this area. Is this one way that security could be improved across the board? Do you think this is a mechanism that could work using insurance as an example?

MR. NOZNESKY: Yes, I can't speak so much for the insurance. I will tell you that from the perspective of our industry, we have looked at trying to help formulate standards, guidelines initially, and then ultimately standards to show that we wanted to take the initiative to protect the systems and that sort of thing, but, no, I am not that familiar with the insurance portion.

MS. MESERVE: Johanna, absent this insurance at this point in time, this kind of coverage, what should a CEO do? How do they protect themselves? Is there some backstop that should be created?

MS. SCHNEIDER: Sure. Well, CEOs clearly have a fiduciary responsibility to protect their employees, to protect their physical assets in any type of a disaster or an event. So they owe it to the shareholders, they owe it to the employees, and that of course is their first and primary responsibility. And to that point, you should all know, every company has continuity plans. They practice those continuity plans, they prepare, they are very well educated. So they know if something were to happen to this company, the employees all over the country – here is how we recover, here is how we connect. So they have, as I said, a fiduciary responsibility.

Beyond that, in the greater sense, what we are really talking about is I think a tremendous economic potential for disaster for this country because if you do not have reinsurance, and if you do not have insurance, and you have a major event, at some point, there will be public pressure for the government to step in to provide that backstop that is necessary. That of course would create a tremendous impact on the economy. There would be deficits; there would be an issue of fairness. And so I think it's only prudent that we all have to come together and try to look at what is the reinsurance market, what is the insurance industry's role?

Florida is a great example. When they started to provide some best practices and some guidelines around rebuilding structures and those structures were up to code, the impact had been dramatically reduced in an area that is frequently impacted like Florida. So I think nationwide, we need to think about those types of strategies.

MS. MESERVE: Would you think that government should have a rainy-day fund at the ready for this sort of catastrophe where they might have to step in?

MS. SCHNEIDER: I think from an economic standpoint, they need it.

MS. MESERVE: In the meantime, Harry, what is a business to do?

MR. OELLRICH: Well, that is an interesting question. I think one of the first things that you need to do, because it's very likely that when push comes to shove, you may not be able to have or you may not be able to secure all of the coverages that you would ultimately need. Therefore I think it behooves every business to really get out there straightaway and assess what their exposures are, and to basically mitigate those however they can.

I mean, this will sound like an advertisement to some degree, but you need to be able to have an advocate on your team. Large companies are able to have either risk departments or a risk manager on staff, and even those major companies use the services of major specialists, brokers, for instance, that will basically come in, will assess your exposures, they work in that space every day; they basically can take a look at what you have, look at your coverages, hand tailor coverages, tell you what you need, and then be able to secure them at an efficient cost. That provides belts and suspenders to some degree in terms of knowing that you have what is available at an effective cost.

The smaller companies and the mid-size companies may not have the luxury of having those specialists on staff, so it becomes even more important for them to be able to bring a professional in who does this for a living 24x7. You can't have your CFO or your general counsel being responsible for all of the insurance decisions within your company.

MS. MESERVE: David, you have been down there in the Gulf Coast looking at it up close. What impact has insurance had, could insurance have in that recovery?

MR. EISNER: Well, when I look at it from an insurance point of view, I look at it a little bit differently from the reinsurance perspective. What I have been seeing in both Mississippi and particularly in New Orleans is an incredible amount of confusion because the insurers all have different policies around what constitutes hurricane damage and what constitutes flood damage. Generally the wind damage is considered covered; the flood damage is not.

People fall into several different categories. One, they are arguing with their insurance company about which it is, and then some of the insurance companies themselves are trying to decide what kind of damage constitutes wind and flood, and anybody down there sort of looking at a destroyed shotgun home with a hole in the ceiling and flood damage in the middle knows, well, the damage was caused by water, so now you have got to figure out whether the water came in the door through the flood, or whether it came into the ceiling.

It becomes a pretty academic exercise, and it's – right now, I think one of the big challenges that a lot of residents are having, and a lot of whole communities are having trying to figure out whether their losses will be covered or not.

MS. MESERVE: We have all had an opportunity to complain, to put some of the issues out on the table. I would like to spend a significant amount of time here trying to come up with some ideas on what we do about it, how we move past this to some kind of action plan. Paul, your organization I think has even come up with some specific things that you want to see the government do, some of the real basics that you think have to be addressed. Would you go over those?

MR. KURTZ: Sure, in the area of IT security, we would like to see a number of things happen, six to be exact: first of all, more leadership. We are starting to see that with the decision to appoint Greg Garcia as the assistant secretary. It's a step in the right direction. He has a good background, good capabilities, so we are happy to see that. Secondly, we want to see sponsorship of prevention and mitigation programs, investment of the insurance market is one. Another one is R&D. Nine-hundred-million-dollar budget of S&T at the Department of Homeland Security – \$20 million dollars goes to cyber-security R&D. That number should be increased over the coming years.

MS. MESERVE: That sort of research is being done elsewhere in the government.

MR. KURTZ: It is done at other agencies or National Science Foundation and DOD, but there is a distinction, there is a difference. DOD does research in this area for its own reasons, and much of that is in the black. In this case it would be very helpful to have research on resilient systems for the broader information infrastructure. After all, everybody, including DOD, rests on the same information infrastructure. So it would be very helpful to see that expanded to the Department of Homeland Security.

The third area is early warning and situational awareness programs, a tighter embrace of the IT ISAC that is responsible for sharing information, the Department developing more fully its own information feeds for actually what is going on information networks. Fourth area – command-and-control procedures in the case of a crisis: Who are we calling up the food chain when we have a problem and when we kind of tip over the top into recovery and reconstitution? Those issues are not clear; the Department has made that clear, but we need hard programs and exercises to address that.

Fifth area, if you will, emergency communications. In other words, today, everything we do in order to respond to a crisis depends upon those information networks. So what if those information networks themselves are under attack? Well, maybe in the absence of a physical attack elsewhere or a natural disaster, they themselves may be under attack. So what is plan B, what is plan C, what is plan D, how are we going to actually communicate amongst critical infrastructures?

And finally, a national information assurance policy - a policy of resilience for our overall information infrastructure. You know, we have our strategy, we have our plans, but we don't have a statement that it is the policy of the United States to have a resilient information infrastructure. We don't have that statement. I don't want to put too much emphasis on that last point because we have lots of plans and lots of strategies.

And I said in the beginning, we need hard programs and hard priorities in this area. And let's start debating those programs as to whether or not there are right ones and wrong ones. And the ones I just listed off, people may have a different opinion. Let's engage in that debate about programs and spending rather a discussion of broad aspirational statements.

MS. MESERVE: David, you seem more or less pleased with the state of play, but do you have any suggestions for further improvements on how to do better?

MR. NOZNESKY: Well, I think a number of things over the last few years have been progressing and are slowly being implemented. I would like to emphasize some of the improvements, some of the positive things that have occurred.

And I think one area in particular that relates to the power industry is the National Infrastructure Protection Plan. I mentioned that earlier. But the reason why I wanted to bring that up is because there is a sector-specific plan that is included in that. And that was I think one of the best examples in the last two or three years to show that public-private partnership, addressing specific plans with good, solid private sector input, good dialogue between the two.

There is the new implementation of the joint field operations, private sector liaison that DHS is going to implement – I think this is very critical because when there is a disaster, it is going to be very critical for that single point of contact, that one coordinator. And for the private sector, I think for all of the sectors in the private sector, I think this is going to be a positive.

The new Homeland Security Information Network, which is started over the last year, year-and-a-half, I think is going to be a positive to getting information out, situational awareness, perhaps early warning. And it's in its infancy, but I think that is an area that is going to continue to be strengthened.

One of the things I mentioned on the telephone – the Department of State many years ago created the Overseas Security Advisory Council, and that has been an outstanding public-private partnership, particularly for U.S. companies doing business overseas. There is an excellent exchange of information, threat information, which is critical to being able to do any kind of risk assessment and manage risk. And I think there is a real place for a domestic security advisory council for companies relating to the Department of Homeland Security or homeland security issues, and now that looks like it's beginning to take off. So I would like to see that as we move forward to develop and mature.

MS. MESERVE: You have mentioned a number of different things, and I wonder if there is room for confusion. Are there in some instances too many possible channels for information to flow that might muddy the picture for you?

MR. NOZNESKY: It could. I do believe, though, that the Department of Homeland Security is trying to coordinate that information, and I think the HSIN, or the Homeland Security Information Network, should help to improve the coordination of information that comes out. We'll see. That is all a work in progress, but certainly that is a factor.

MS. MESERVE: Coordination, one of your big issues.

MR. NOZNESKY: Right.

MS. MESERVE: Tell us how we address it. What is the plan?

MR. EISNER: Well, I think the most important thing is to be able to operate at several different levels. It is really important for us to build the relationships, improve the National Response Plan so that we all understand what we are going to try to do together to make sure that the business community is coming together, that the non-profit community, that the government all have these plans.

But at the same time, it's really important to recognize that you can't use this plan as a bottleneck. It can't be that if someone says I can fix that problem that they have to go through this elaborate process that has been prescribed. An awful lot – and when I was at AOL during September 11th, one of the things that we did that was most effective – the Blackberries were working; the phones and the radios weren't. We just made thousands of Blackberries available to the police officers and fireman, and then later we worried about making sure that all of the managers and the folks understood it.

So it's really important to be able to operate both at that sort of planning-coordination level to maximize the chance that your plans are going to have an impact, but not create a culture where businesses or private citizens or government somehow believe that the plan itself is going to fix everything because I think one of the things that we learned is as strong and as good and as well prepared as we are, there is going to be things that we are not ready for, and something like catastrophe will require all of us to use all of our best assets.

And we have to be really careful – I think one of the big mistakes we made was we felt that because we were all signatories of the National Response Plan, and because we knew this National Response Plan could hit certain benchmarks, we kind of over-relied on it.

MS. MESERVE: Did it stifle improvisation in some respects? I mean, the Coast Guard has been lauded for going off on its own and saying, "plans be damned," we are going to go out and rescue lives. Were there other people who you think held back, didn't do what they might have seen needed to be done because they were afraid of not following that plan to the letter?

MR. EISNER: Well, I think it was less about not following the plan to the letter and a lot of folks being insecure about who had the ability to say okay to something. And as soon as folks started worrying that we didn't know who could say okay, then you had people that were not able to get – companies not able to provide their capacity. You had volunteers not able to get what they needed done, and you had mayors and folks on the ground not able to get people to give them a thumbs-up because no one knew well enough who could say okay.

I think that is one of the things we have got to get right. We left it a little bit this time to be a struggle between national and state control over some of the big questions. I think we will see the next National Response Plan be a little bit clearer and more prescriptive that in this kind of situation it will be a state call; in this kind of situation it will be a federal call.

MS. MESERVE: I was going to ask you about the rewrite of the plan. Are there some specific things you want to see in there?

MR. EISNER: Well, of course from a corporation's point of view, we have a pretty narrow focus; we are a signatory of the National Response Plan. We just want to make sure that we give as much capacity to particularly the Red Cross, the National Volunteer Organizations Active in Disasters, and corporation assets so that we can move even more people and more assets faster. We have got in the course of a year 35,000 participants in AmeriCorp, Senior Corps, and Vista into the Gulf. We think we could have done even better, and we think that we could have helped Catholic Charities and Red Cross and Salvation Army be even more effective.

And even though those are operating on what you might think of as a different side than critical infrastructure, when you are on the ground in these communities and you see the mayors making decisions, they are literally – they have got a pool of people, and they are making horrible choices about whether they are going to be focusing on getting the water going, or whether they are going to be taking care of a hospital crisis. So when you are able to get those kinds of people on the ground managing things, it frees up capacity to be able to make some of the critical infrastructure work.

MS. MESERVE: Johanna, what is your wish list?

MS. SCHNEIDER: Well, back to information is king, we amassed a tremendous amount of information on the corporate side following the tsunami, Hurricane Katrina, Rita, Wilma, Stan. Next week we will be announcing a website, a public website, www.respondtodisaster.org. We have taken all of this information and put it into the website. It explains to the average – no acronyms – to the average reader what is the role of the Federal government in the midst of a disaster, what is the role of a state and local government, what is the role of a corporation, what is the role of an NGO. We list in an encyclopedic form, every NGO, what they do, who to contact, what specific role they have to play. So we think this will help small businesses, large businesses. This is for the public to become educated about disasters.

Again, back to your point, precisely, if you can become educated prior to the day of the disaster, you will perform much more efficiently during the disaster. So first and foremost, we are trying to provide a public service through the website, and then secondly we are trying to coordinate all corporations across the board so they have an input through the Roundtable so in the event of a catastrophic disaster, they can leverage each other's expertise, go through the Roundtable, and get to the government.

MS. MESERVE: Will competitors cooperate in this field?

MS. SCHNEIDER: That is a great question, and of course antitrust is always on the minds of every corporate lawyer, and we have, and are continuing to work through – but, yes, I think the bottom line is the CEOs have told us they think they have worked through it, and, yes, they can both coordinate and collaborate.

MS. MESERVE: Harry, you have told us what you want. You want that data hidden somewhere in the bowels of government.

MR. OELLRICH: Right.

MS. MESERVE: Have you got an action plan? Have you got some specific concrete steps, ideas on how to grab hold of that and pull it out?

MR. OELLRICH: Well, I think the place that it really all starts from is by staying away from the trap that you can all fall into with many sectors and with many industries, and that is just saying “the insurance industry,” or “the reinsurance industry.” What you have in that space is an incredible diversity of different companies, different corporate cultures, different goals, different objectives. But what I think you'll find when you go out and talk to the senior executives of those companies, they all recognize that they are part of critical infrastructure themselves and that their goal is to be part of the solution as opposed to part of the problem.

And if you can tie into specific individuals that get certain issues, and be able to know that they have counterparts within government that can work certain issues with them, that is going to go a long way towards being able to get enough specificity to be able to maybe drill down and get at some of what we think is part of the answer.

MS. MESERVE: A lot of individuals and a lot of local governments came to the conclusion after Katrina that they had to look out for themselves, that they just couldn't count on government to do it for them. Have any of you come to that conclusion?

MS. SCHNEIDER: Absolutely. If you can't help, get out of the way. I mean, that is our motto. Fran Townsend put it in her report frankly.

MR. EISNER: I don't see it as an either/or. I think it's an “and.” If you look at most of the communities and what is happening with the faith-based organizations who

were rebuilding their neighborhood, they are looking for the support that they can get from their government, but they are certainly not waiting on government to make their decisions; they are going about rebuilding their communities, putting the assets that they can. But many of these neighborhoods still don't have electricity, power, water, and they are still rebuilding, mucking out the homes, getting them ready.

And I should note, we are spending a lot of time talking about the future. We still have incredible needs in Katrina, and they are right now at the state where they can best absorb volunteers, and in particular volunteers in the kinds of critical infrastructure areas we are talking about: electricians, plumber, carpenters, teachers, healthcare workers. If anybody know folks or can take time go onto www.volunteer.gov. Right now is when the Katrina folks need you.

MS. MESERVE: Another ad here. Take advantage of it.

Well, we have been talking about government, and I think most of us sort of conceive of government as the administration, the bureaucracy, but what about the Congress? Are there things this Congress has to do, either in terms of action, in terms of oversight? Paul, have you got any thoughts on that?

MR. KURTZ: Yeah, I think there are things they can do and that they are doing. I think security has been identified as a major election-year issue by both the Democrats and Republicans, we see movement on the Hill on chemical site security, port security, all of those issues that the Congress is trying to push ahead. And I think that is important. And rather than at the end of the session, I would rather see it at the beginning. But in the area of IT security, I think Congress is struggling a bit. And part of that is explainable because we have multiple committees with jurisdiction information systems. You can't say it's all energy and commerce or government reform and financial services. In fact, multiple committees have jurisdiction.

And for example right now a huge problem that Americans are facing – 90-some million Americans have had their personal information put at risk over the past year-and-a-half, yet we don't have a bill out of Congress to provide the basis of secure and sensitive personal information outside the financial services space, which is already securing that information. Congress is not going to act on that bill this year. It's unfortunate. And that feeds into a level of confidence and distrust in the Internet.

MS. MESERVE: How do they get pushed into action? What could do it?

MR. KURTZ: Well, I think one, we all need to be vocal. Industries need to be vocal and of course constituents need to be vocal in this space and reach up to their members of Congress and let them know that they do have concerns about the information infrastructure. We have done some polling ourselves, and when you ask people about how well the information infrastructure is working and how secure it is, you get two different results. They all think it's working okay, you're getting more of the 60-percent mark, but when you talk about how safe and secure it is, they are down in the 10s

and 20s. That is an indicator; there is some angst out there among people, and they should start talking to their elected representatives and focus more attention on this issue.

MS. MESERVE: When it comes to chemical plant security, there has been talk of regulation. In your sphere, is regulation productive? Would that improve things – in furthering security of the private infrastructure as something that is needed, or as something that is not?

MR. NOZNESKY: Well, I think that, first, any regulation that is going to be out there needs to have private sector input and it has to be reasonable and appropriate. I look more toward the industry, our industry, to formulate best practices. As I indicated before, right after 9/11, and in fact, even before 9/11, I looked to our industry for company security standards, both cyber and physical. I think another good example – Secretary Foresman mentioned it earlier-- is collaboration between private sector companies themselves, not only with the federal government.

Recently there was an announcement that the Edison Electric Institute had coordinated a spare-parts inventory for major disasters, which is a collaboration between the companies that is going to be very important as we go forward. So I look more for the industry and the companies to take responsibility and to establish the correct best practices and so on.

MS. MESERVE: Okay, great. Anything else any of you want to throw into the mix here before we wrap it up?

MS. SCHNEIDER: Two issues, and I am supporting what you have just said, which is that Congress really needs to focus on port security and cyber security. These are areas that have been lacking in terms of a bipartisan consensus. And if I could put two things on the radar screen for the next year and the next Congress, it would be those two issues.

MS. MESERVE: Great. John, I think you were going to take all of this and sum it up. I want to thank you all. You are all terrific.

MR. MCCARTHY: Thank you very much. A hand for the panel. (Applause.) Thank you.

The challenge to sum up this group – one thing, as a former Coast Guardsman who did cyber security in the government, I am all with you on that legislative initiative. Without going through my prepared remarks, let me hit a couple of themes. One very significant theme that I heard from this group is I think we are at a critical moment in our evolutionary step along the emergency-management / preparedness continuum between the public and private sector.

And that step is moving from trusted people, trusted individual relationships to trust the processes for a whole bunch of reasons – the idea that you can replicate the

relationship when things change, or in the case in New York, many of the individuals in these key relationships were involved in the catastrophe, and unfortunately perished instantly. We saw in New Orleans people who were part of the response process not show up. So we have to look at the scale and scope and intensity of an incident driving the notion that we need reliable processes to go to, so no matter what happens, on either end of that process, the public or private sector, or academe, or whatever, the news media, you can enter the process with some assurance that you will have a more positive outcome on the other side.

George Forseman I think summed it up with “teachable moment.” I think that was at the crux of where he was going. And that was a consistent theme you heard across all, the idea of the CEOs of major corporations stepping out and saying, with all due respect, we are not going to wait for the government. We have to understand and teach ourselves, and if we are better prepared then we can go and present a unified front to the public sector when they need us. And I think that is a very important thing.

Johanna, you get the award for the best quote or clip: “dwell on the solution.” I think that needs to be an underlying theme of this entire process. “Lead, follow, or get out of the way” is one of my favorite expressions. I want to thank the panel again. Jeanne did an outstanding job. Thank you very much for bringing out this insight from this great group. And thank you all for attending.

(Applause.)

(END)